

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 519.7

<https://doi.org/10.26907/2541-7746.2025.2.213-226>

2-адическая сложность бинарных последовательностей Динга – Хеллесета с периодом pq

В.А. Едемский*Новгородский государственный университет им. Ярослава Мудрого, г. Великий Новгород, Россия**vladimir.edemsky@novsu.ru***Аннотация**

Предложен метод анализа 2-адической сложности бинарных обобщенных циклотомических последовательностей с периодом pq . 2-адическая сложность, наряду с линейной сложностью, является важной характеристикой непредсказуемости последовательностей. Метод основан на использовании обобщенных гауссовых периодов различных порядков по простым модулям p и q . Оценена 2-адическая сложность обобщенных циклотомических последовательностей Динга – Хеллесета второго, четвертого и шестого порядков с высокой линейной сложностью. Показано, что рассмотренные последовательности обладают большой 2-адической сложностью, достаточной для отражения атак посредством алгоритма рациональной аппроксимации. Обобщены предыдущие результаты, полученные для последовательностей второго порядка.

Рассмотренный метод может быть использован для последовательностей другого вида, которые определяются посредством использования обобщенных циклотомических классов разных порядков. Его также можно применять для анализа m -адической сложности как бинарных, так и небинарных последовательностей, например, четвертичных.

Ключевые слова: 2-адическая сложность, обобщенная циклотомическая последовательность

Благодарности. Исследование выполнено при финансовой поддержке Российского научного фонда, проект № 24-21-00442.

Для цитирования: Едемский В.А. 2-адическая сложность бинарных последовательностей Динга – Хеллесета с периодом pq // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2025. Т. 167, кн. 2. С. 213–226. <https://doi.org/10.26907/2541-7746.2025.2.213-226>.

ORIGINAL ARTICLE

<https://doi.org/10.26907/2541-7746.2025.2.213-226>

2-Adic complexity of Ding–Helleseeth binary sequences with period pq

V.A. Edemskiy

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

vladimir.edemsky@novsu.ru

Abstract

A method is proposed to analyze the 2-adic complexity of generalized cyclotomic binary sequences with period pq . Along with linear complexity, 2-adic complexity serves as an important measure of sequence unpredictability. The method is based on generalized Gaussian periods of various orders using the prime modules p and q . The 2-adic complexity of Ding–Helleseeth generalized cyclotomic sequences of orders two, four, and six with high linear complexity is estimated. The analysis shows that these sequences have high 2-adic complexity, which is sufficient to resist attacks using the rational approximation algorithm. Previous results obtained for the sequences of order two are summarized. The proposed method can be applied to a different type of sequences defined using generalized cyclotomic classes of various orders, as well as to investigate the m -adic complexity of both binary and non-binary sequences, such as quaternary sequences.

Keywords: 2-adic complexity, generalized cyclotomic sequences

Acknowledgments. This study was supported by the Russian Science Foundation (project no. 24-21-00442).

For citation: Edemskiy V.A. 2-Adic complexity of Ding–Helleseeth binary sequences with period pq . *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2025, vol. 167, no. 2, pp. 213–226. <https://doi.org/10.26907/2541-7746.2025.2.213-226>. (In Russian)

Введение

Для оценки непредсказуемости псевдослучайных последовательностей применяют различные виды сложностей, наиболее известной из которых является линейная. 2-адическая сложность, как мера непредсказуемости последовательностей, была предложена в [1] для оценки последовательностей, синтезируемых регистром сдвига с обратной связью по переносу. Свойства 2-адической сложности и различные алгоритмы её вычисления изложены в [2]. Согласно алгоритму рациональной аппроксимации для нахождения последовательности с 2-адической сложностью m достаточно $2m$ последовательных членов последовательности, то есть для «хороших» периодических последовательностей их 2-адическая сложность должна быть больше половины периода. Таким образом, желательно, чтобы

последовательности имели не только высокую линейную сложность, но и 2-адическую. Последнее замечание послужило причиной появления серии статей, посвященных исследованию 2-адической сложности бинарных последовательностей, обладающих высокой линейной сложностью. Так, в [3–5] определена 2-адическая сложность последовательностей с идеальной или почти идеальной автокорреляцией, в [6–8] – чередующихся последовательностей, а в [9–12] – ряда обобщенных циклотомических последовательностей, в частности, в [13, 14] оценена 2-адическая сложность последовательностей Динга – Хеллесета второго порядка с периодом pq , где p и q – различные простые числа, при ограничениях на p и q . Линейная сложность таких последовательностей изучена ранее.

В настоящий момент известно несколько теоретических способов исследования 2-адической сложности последовательности, основанных на использовании: автокорреляции последовательности; циклического определителя, составленного из значений дискретного преобразования Фурье последовательности; обобщенных гауссовых периодов для последовательностей простого периода или удвоенного [3, 12, 15]. В настоящей статье предложено распространение последнего подхода на последовательности с периодом pq , где p и q – различные простые числа. Для иллюстрации метода обобщим результаты из [13, 14] без ограничений на p, q , а также докажем, что обобщенные циклотомические последовательности Динга – Хеллесета четвертого и шестого порядков обладают высокой 2-адической сложностью. Предложенный метод исследования 2-адической сложности можно использовать для изучения 2-адической сложности модернизированных последовательностей Динга – Хеллесета [16], а также m -адической сложности подобных последовательностей для $m > 2$.

1. Обобщенные циклотомические последовательности

Прежде всего, напомним определение обобщенных циклотомических классов Динга – Хеллесета по модулю pq [17].

Пусть p и q – различные нечетные простые числа, $d = \text{НОД}(p-1, q-1)$ и $e = (p-1)(q-1)/d$. Так как p и q – простые числа, то всегда существует общий примитивный корень g по модулям p и q , его порядок по модулю pq равен e [18].

Обозначим через H_i и G_i циклотомические классы порядка d по модулям p и q соответственно, то есть

$$H_i = \left\{ g^{i+dj} \bmod p \mid j = 0, 1, \dots, \frac{p-1}{d} - 1 \right\} \text{ и } G_i = \left\{ g^{i+dj} \bmod q \mid j = 0, 1, \dots, \frac{q-1}{d} - 1 \right\}, \\ i = 0, 1, \dots, d-1.$$

Тогда справедливы разбиения

$$\mathbb{Z}_p = \bigcup_{i=0}^{d-1} H_i \cup \{0\} \text{ и } \mathbb{Z}_q = \bigcup_{i=0}^{d-1} G_i \cup \{0\}.$$

Согласно китайской теореме об остатках существует такое число $x \in \mathbb{Z}$, что $x \equiv g \pmod{p}$, $x \equiv 1 \pmod{q}$. Обобщенные циклотомические классы Динга – Хеллесета порядка d по модулю pq определяются следующим образом:

$$D_i = \left\{ g^{i+jd} x^t \bmod pq \mid j = 0, 1, \dots, \frac{e}{d} - 1, t = 0, 1, \dots, d-1 \right\}, \quad i = 0, 1, \dots, d-1.$$

Обозначим через $\mathbb{Z}_{pq}^*$ группу обратимых элементов $\mathbb{Z}_{pq}$, где $\mathbb{Z}_{pq}$ – кольцо классов вычетов по модулю pq . Пусть $P = \{p, 2p, \dots, (q-1)p\}$ и $Q = \{q, 2q, \dots, (p-1)q\}$. Тогда

$$\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{d-1} D_i \text{ и } \mathbb{Z}_{pq} = \bigcup_{i=0}^{d-1} D_i \cup P \cup Q \cup \{0\}.$$

Определим последовательность Динга–Хеллесета s с периодом pq по формуле

$$s_i = \begin{cases} 1, & \text{если } i \bmod pq \in \bigcup_{i=d/2}^{d-1} D_i \cup C, \\ 0 & \text{иначе,} \end{cases} \quad (1)$$

где $C = Q$, или $C = P$, или $C = \bigcup_{i=d/2}^{d-1} qH_i \cup \bigcup_{i=d/2}^{d-1} pG_i$ [13, 14].

В завершение раздела напомним, что 2-адическая сложность $\Phi_2(s)$ последовательности s с периодом pq , согласно [2], может быть вычислена по формуле

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

где $S(x) = \sum_{i=0}^{pq-1} s_i x^i \in \mathbb{Z}[x]$ – многочлен последовательности s . Таким образом, для нахождения 2-адической сложности достаточно изучить наибольший общий делитель двух чисел $S(2)$ и $2^{pq} - 1$. В данном случае, при определении последовательности посредством D_i , важны свойства сумм $\sum_{j \in D_i} 2^j$. В следующем разделе покажем, как классы вычетов D_i связаны с циклотомическими классами порядка d по модулям p , q , и рассмотрим метод вычисления этих сумм.

2. Метод анализа 2-адической сложности

Кольцо классов вычетов $\mathbb{Z}_{pq}$ изоморфно прямому произведению $\mathbb{Z}_p \times \mathbb{Z}_q$ относительно изоморфизма $f(t) = (t \bmod p, t \bmod q)$ [18]. Пусть $F_{i,j} = f^{-1}(H_i \times G_j)$, $i, j = 0, 1, \dots, d-1$. Следовательно,

$$\mathbb{Z}_{pq}^* = \bigcup_{i=0}^{d-1} \bigcup_{j=0}^{d-1} F_{i,j} \text{ и } \mathbb{Z}_{pq} = \bigcup_{i=0}^{d-1} \bigcup_{j=0}^{d-1} F_{i,j} \cup \bigcup_{i=0}^{d-1} qH_i \cup \bigcup_{i=0}^{d-1} pG_i \cup \{0\}.$$

Используя определения множеств D_i и $F_{i,j}$, получим следующее утверждение.

Лемма 1. Для $i = 0, 1, \dots, d-1$ имеем $D_i = \bigcup_{j=0}^{d-1} F_{j,i}$.

Таким образом, обобщенная циклотомическая последовательность Динга–Хеллесета с периодом pq может быть определена с использованием множеств $F_{i,j}, H_i, G_i$. Следовательно, согласно формуле (2) для анализа 2-адической сложности таких последовательностей достаточно изучить суммы степеней 2, когда показатели степеней принадлежат множествам $F_{i,j}, H_i, G_i$.

Определим вспомогательные многочлены $S_i^{(d)}(x) = \sum_{u \in H_i} x^u$ и $T_i^{(d)}(x) = \sum_{v \in G_i} x^v$ для всех $i = 0, 1, \dots, d-1$. Далее индексы многочленов $S_i^{(d)}(x)$ и $T_i^{(d)}(x)$ всегда будем вычислять по модулю d . Следующие сравнения непосредственно вытекают из определений вспомогательных многочленов и классов вычетов.

Лемма 2. Пусть u, v – натуральные числа, $\text{НОД}(u, p) = 1$ и $\text{НОД}(v, q) = 1$. Тогда

$$A. S_i^{(d)}(2^{ug^j}) \equiv S_{i+j}^{(d)}(2^u) \pmod{2^{up} - 1};$$

$$B. S_0^{(d)}(2^u) + S_1^{(d)}(2^u) + \dots + S_{d-1}^{(d)}(2^u) \equiv -1 \pmod{(2^{up} - 1)/(2^u - 1)};$$

$$C. T_i^{(d)}(2^{vg^j}) \equiv T_{i+j}^{(d)}(2^v) \pmod{2^{vq} - 1};$$

$$D. T_0^{(d)}(2^v) + T_1^{(d)}(2^v) + \dots + T_{d-1}^{(d)}(2^v) \equiv -1 \pmod{(2^{vq} - 1)/(2^v - 1)}.$$

Так как числа p и q взаимно просты, то всегда существуют такие целые числа a и b , что $1 \equiv aq + bp \pmod{pq}$, $0 < a < p$, $0 < b < q$.

Лемма 3. Пусть $i, j = 0, 1, \dots, d-1$. Тогда $\sum_{u \in F_{i,j}} 2^u \equiv S_i^{(d)}(2^{aq}) T_j^{(d)}(2^{bp}) \pmod{2^{pq} - 1}$.

Доказательство. По определению $F_{i,j}$ получим, что

$$\sum_{u \in F_{i,j}} 2^u \equiv \sum_{u \in F_{i,j}} 2^{u_{aq}} 2^{u_{bp}} \pmod{2^{pq} - 1}.$$

Тогда

$$\sum_{u \in F_{i,j}} 2^u \equiv \sum_{u \in H_i} 2^{u_{aq}} \sum_{u \in G_j} 2^{u_{bp}} \equiv S_i^{(d)}(2^{aq}) T_j^{(d)}(2^{bp}) \pmod{2^{pq} - 1}. \quad \square$$

Следствие 1. Если последовательность s определена по формуле (1), то

$$S(2) \equiv \sum_{i=0}^{d-1} S_i^{(d)}(2^{aq}) \sum_{j=d/2}^{d-1} T_j^{(d)}(2^{bp}) + \sum_{i \in C} 2^i \pmod{2^{pq} - 1}.$$

Это утверждение следует непосредственно из леммы 3 и определения последовательности.

Лемма 4. Пусть $P_i = pG_i$, $Q_i = qH_i$, $i = 0, 1, \dots, d-1$. Тогда

$$\sum_{u \in P_i} 2^u \equiv T_i^{(d)}(2^p) \pmod{2^{pq} - 1} \quad \text{и} \quad \sum_{u \in Q_j} 2^u \equiv S_j^{(d)}(2^q) \pmod{2^{pq} - 1}.$$

Лемма 4 может быть доказана тем же самым способом, что и лемма 3.

Согласно формуле (2) для анализа 2-адической сложности достаточно изучить $\text{НОД}(S(2), 2^{pq} - 1)$. Так как p и q – простые числа, то справедливо разложение

$$2^{pq} - 1 = (2^p - 1) \cdot (2^q - 1) \cdot \frac{2^{pq} - 1}{(2^p - 1)(2^q - 1)},$$

и $\text{НОД}(2^p - 1, 2^q - 1) = 1$. Применив следствие 1 и лемму 2, получим следующие сравнения, представленные в лемме 5.

Лемма 5. Пусть последовательность Динга–Хеллесета s определена по формуле (1)

$$u \ U^{(d)}(2) = \sum_{j=d/2}^{d-1} T_j^{(d)}(2^{bp}). \text{ Тогда}$$

$$A. \text{ НОД}(S(2), 2^p - 1) = \text{НОД}\left(2^p - 1, -(q-1)/2 + \sum_{i \in C} 2^i\right);$$

$$B. \text{ НОД}(S(2), 2^q - 1) = \text{НОД}\left(2^q - 1, (p-1)U^{(d)}(2) + \sum_{i \in C} 2^i\right);$$

$$C. \text{ НОД}\left(S(2), \frac{2^{pq}-1}{(2^p-1)(2^q-1)}\right) = \text{НОД}\left(\frac{2^{pq}-1}{(2^p-1)(2^q-1)}, -U^{(d)}(2) + \sum_{i \in C} 2^i\right).$$

Таким образом, в силу лемм 1–5 для анализа 2-адической сложности последовательностей с периодом pq можно использовать свойства многочленов $S_i^{(d)}(x)$ и $T_i^{(d)}(x)$, которые рассматривались ранее в [12, 19, 20]. Применив их в следующих разделах, получим оценку 2-адической сложности последовательностей.

В заключение раздела заметим, что утверждения лемм 2–4 останутся верными, если взять циклотомические классы H_i и G_j разных порядков, а также, когда d – делитель $\text{НОД}(p-1, q-1)$, не равный $\text{НОД}(p-1, q-1)$. Таким образом, данный подход можно использовать и для других обобщенных циклотомических последовательностей с периодом pq , в частности, для модернизированных последовательностей Динга–Хеллесета, предложенных в [16].

3. 2-адическая сложность последовательностей

Изучим 2-адическую сложность обобщенных циклотомических последовательностей Динга–Хеллесета второго, четвертого и шестого порядков.

3.1. Последовательности второго порядка. Пусть $d = 2$ и последовательность s с периодом pq определена по формуле

$$s_i = \begin{cases} 1, & \text{если } i \bmod pq \in D_1 \cup Q, \\ 0 & \text{иначе.} \end{cases} \quad (3)$$

Для исследования 2-адической сложности последовательностей второго порядка используем свойства многочленов $T_0^{(2)}(x)$, $T_1^{(2)}(x)$, полученные в [19]. Согласно [19] справедливы следующие сравнения:

$$\left(T_0^{(2)}(2^u) - T_1^{(2)}(2^u)\right)^2 \equiv \left(\frac{-1}{q}\right) q \pmod{(2^{uq} - 1)/(2^u - 1)}, \quad (4)$$

где $\left(\frac{-1}{q}\right)$ – символ Лежандра, $\text{НОД}(u, q) = 1$. По лемме 1

$$\left(2T_i^{(2)}(2^u) + 1\right)^2 \equiv \left(\frac{-1}{q}\right) q \pmod{(2^{uq} - 1)/(2^u - 1)}, \quad i = 0, 1. \quad (5)$$

Аналогичные сравнения справедливы для многочлена $S_i^{(2)}(x)$.

Теорема 1. Пусть последовательность s с периодом pq определена по формуле (3). Тогда

$$\Phi_2(s) = \log_2 \left(\frac{2^{pq} - 1}{d_1 d_2} + 1 \right),$$

где $d_1 = \text{НОД}(2^p - 1, (q + 1)/2)$ и $d_2 = \text{НОД}(2^q - 1, p - 1)$. В частности,

$$\Phi_2(s) \geq pq - \log_2(\max(p, q)).$$

Доказательство. По условию $C = Q$. Тогда

$$\sum_{i \in C} 2^i \equiv -1 \pmod{2^p - 1}, \quad \sum_{i \in C} 2^i \equiv p - 1 \pmod{2^q - 1}, \quad \sum_{i \in C} 2^i \equiv -1 \pmod{\frac{2^{pq} - 1}{(2^p - 1)(2^q - 1)}}.$$

Следовательно, согласно лемме 5

$$d_1 = \text{НОД}(S(2), 2^p - 1) = \text{НОД}(2^p - 1, (q + 1)/2), \\ d_2 = \text{НОД}(S(2), 2^q - 1) = \text{НОД}(2^q - 1, (p - 1)T_1^{(2)}(2^{bp}) + (p - 1)).$$

Так как $\text{НОД}(2^q - 1, T_1^{(2)}(2^{bp}) + 1) = 1$ в силу соотношения (5) и малой теоремы Ферма, то $\text{НОД}(S(2), 2^q - 1) = \text{НОД}(2^q - 1, p - 1)$.

Наконец, если $d_3 > 1$ делит $\text{НОД}\left(S(2), \frac{2^{pq} - 1}{(2^p - 1)(2^q - 1)}\right)$, то опять же по лемме 5 имеет место сравнение $T_1^{(2)}(2^{bp}) \equiv 1 \pmod{d_3}$. По формуле (5) последнее сравнение невозможно, значит, $d_3 = 1$. А так как $\text{НОД}(2^p - 1, 2^q - 1) = 1$, то $d_1 d_2 \leq \max((q - 1)/2, p - 1)$. Это замечание завершает доказательство теоремы 1 в силу формулы (2). $\square$

В частном случае, когда $q = p + 2$, значения $d_1 = d_2 = 1$ по малой теореме Ферма и $\Phi_2(s) = pq$, что было показано в [13]. Отметим, что в общем случае d_1 или d_2 могут быть больше единицы, например, имеем $d_1 = 7$, когда $p = 3$ и $q = 13$ или $p = 3$ и $q = 41$; для $p = 29$ и $q = 3$ значение $d_2 = 7$, а если $p = 47$ и $q = 11$, то значение $d_2 = 23$.

2-адическая сложность последовательности s , определенной по правилу (1) для $d = 2$ и $C = P$, изучена в [19].

Рассмотрим ещё один вариант определения последовательности Динга – Хеллесета второго порядка [14]. Как уже отмечалось во введении, достаточно показать, что 2-адическая сложность последовательности больше половины её периода, поэтому далее ограничимся только её оценкой.

Пусть последовательность s с периодом pq определена по формуле

$$s_i = \begin{cases} 1, & \text{если } i \bmod pq \in D_1 \cup qH_1 \cup pG_1, \\ 0 & \text{иначе.} \end{cases} \quad (6)$$

Теорема 2. Если последовательность s с периодом pq определена по формуле (6), то $\Phi_2(s) \geq pq - 4 \log_2 p - 3 \log_2 q$.

Доказательство. Если последовательность определена по формуле (6), то $C = qH_1 \cup pG_1$ и $\sum_{i \in C} 2^i = S_1^{(2)}(2^q) + T_1^{(2)}(2^p)$. Тогда по лемме 5 (А) и формуле (5) имеем

$\text{НОД}(S(2), 2^p - 1) = \text{НОД}(2^p - 1, S_1^{(2)}(2^q)) = 1$. Далее, если $d_2 = \text{НОД}(S(2), 2^q - 1)$, то по лемме 5 (В) получим сравнение $0 \equiv (p-1)T_1^{(2)}(2^{bp}) + T_1^{(2)}(2^p)/2 + (p-1)/2 \pmod{d_2}$.

Если $b \in G_0$, то $pT_1^{(2)}(2^p) \equiv -(p-1)/2 \pmod{d_2}$ или $p(2T_1^{(2)}(2^p) + 1) \equiv 1 \pmod{2d_2}$. Тогда $p^2 \left(\frac{-1}{q}\right) q \equiv 1 \pmod{4d_2}$ и $d_2 < (1 + p^2q)/4$.

Если же $b \in G_1$, то $(p-2)T_1^{(2)}(2^p) \equiv (p-3)/2 \pmod{d_2}$, $(p-2)^2 \left(\frac{-1}{q}\right) q \equiv 1 \pmod{4d_2}$. Значит, всегда $d_2 < (1 + p^2q)/4$.

Пусть $d_3 = \text{НОД}\left(S(2), \frac{2^{pq}-1}{(2^p-1)(2^q-1)}\right)$. В этом случае согласно лемме 5 (С)

$$0 \equiv -T_1^{(2)}(2^{bp}) + S_1^{(2)}(2^q) + T_1^{(2)}(2^p) \pmod{d_3}.$$

Используя два раза соотношение (5), получим, что $4d_3 < q^2 + q(p+1)/2 + (p-1)^2/16$.

Таким образом, заведомо $d_2d_3 < p^4q^3$, что доказывает теорему 2. $\square$

2-адическая сложность последовательности s оценена в [14], когда $p \equiv q \equiv 3 \pmod{4}$. Заметим, что если $p \not\equiv q \equiv 3 \pmod{4}$, то d_3 может быть не равным единице, как в [14], например, $d_3 = 71$ для $p = 5$, $q = 7$. Но если $b \in G_0$, то $d_3 = 1$. Если $p = 67$, $q = 3$, то $d_2 = 7$, и $d_2 = 23$, если $p = 43$, $q = 11$. Метод, предложенный нами, проще, чем в [14], а оценка d_2 лучше.

3.2. Последовательности четвертого порядка. Исследуем 2-адическую сложность бинарных последовательностей Динга–Хеллесета четвертого порядка. Пусть $d = 4$ и последовательность s определена по правилу

$$s_i = \begin{cases} 1, & \text{если } i \bmod pq \in D_2 \cup D_3 \cup Q, \\ 0 & \text{иначе.} \end{cases} \quad (7)$$

Используем свойства многочленов $T_i^{(4)}(x)$ и $U^{(4)}(x) = T_2^{(4)}(x) + T_3^{(4)}(x)$. В силу сравнения $q \equiv 1 \pmod{4}$ существуют такие целые числа z, y , что $q = z^2 + 4y^2$, $z \equiv 1 \pmod{4}$. Тогда

$$(U^{(4)}(2^u))^2 + U^{(4)}(2^u) \equiv (q-1)/4 + y(T_0^{(2)}(2^u) - T_1^{(2)}(2^u))/2 \pmod{(2^{uq}-1)/(2^u-1)}, \quad (8)$$

где $\text{НОД}(u, q) = 1$.

Теорема 3. Пусть последовательность s с периодом pq определена по формуле (7). Тогда

$$\Phi_2(s) = \log_2 \left(\frac{2^{pq}-1}{d_1d_2} + 1 \right),$$

где $d_1 = \text{НОД}(2^p - 1, (q+1)/2)$ и $d_2 = \text{НОД}(2^q - 1, p-1)$. В частности,

$$\Phi_2(s) \geq pq - \log_2(\max(p, q)).$$

Доказательство. Как и при доказательстве теоремы 1, получим

$$\text{НОД}(S(2), 2^p - 1) = \text{НОД}(2^p - 1, (q+1)/2).$$

Пусть d_2 делит $\text{НОД}(S(2), 2^q - 1)$, тогда согласно лемме 5 справедливо сравнение

$$(p-1)U^{(4)}(2^{bp}) + (p-1) \equiv 0 \pmod{d_2}.$$

Покажем, что $U^{(4)}(2^{bp}) \not\equiv -1 \pmod{d_2}$.

Предположим противное. В этом случае из сравнений (8) и (4) следует

$$y^2q/4 \equiv (q-1)^2/16 \pmod{d_3} \quad \text{или} \quad (z^2q - 2q + 1)/16 \equiv 0 \pmod{d_2}.$$

Так как q – простое число, то по малой теореме Ферма имеем $d_2 = 1 + 2tq$, $t \in \mathbb{Z}$. Умножив последнее сравнение на $2t$, получим $-(z^2 - 2) + 2t \equiv 0 \pmod{d_2}$. Значит, $z^2 - 2 = 2t$. Пришли к противоречию, так как z – нечетное число. Следовательно,

$$\text{НОД}(S(2), 2^q - 1) = \text{НОД}(2^q - 1, p - 1).$$

Положим $d_3 = \text{НОД}\left(S(2), \frac{2^{pq}-1}{(2^p-1)(2^q-1)}\right)$, тогда согласно лемме 5 (С)

$$U^{(4)}(2^{bp}) \equiv -1 \pmod{d_3}.$$

Используя сравнения (8) и (4), получим

$$y^2q/4 \equiv (q-1)^2/16 \pmod{d_3} \quad \text{или} \quad (z^2q - 2q + 1)/16 \equiv 0 \pmod{d_3}.$$

Если d_3 делит $2^p - 1$ и $\frac{2^{pq}-1}{(2^p-1)(2^q-1)} = 1 + 2^p + \dots + 2^{(q-1)p}$, то $d_3 = q$, что невозможно по вышедоказанному. Аналогично, если d_3 делит $2^q - 1$ и $\frac{2^{pq}-1}{(2^p-1)(2^q-1)}$, то $d_3 = p$, что также невозможно. Следовательно, порядок 2 по модулю d_3 равен pq , и по малой теореме Ферма $d_3 = 1 + 2tpq$. Тогда, рассуждая, как и при оценке d_2 , получим, что $d_3 = 1$. $\square$

Пусть теперь последовательность s определена по правилу

$$s_i = \begin{cases} 1, & \text{если } i \bmod pq \in D_2 \cup D_3 \cup P, \\ 0 & \text{иначе.} \end{cases} \quad (9)$$

Теорема 4. Если последовательность s с периодом pq определена по формуле (9), то $\Phi_2(s) \geq pq - 4 \log_2 p - 3 \log_2 q$.

Доказательство. Рассуждая, как при доказательстве теоремы 3, получим

$$\text{НОД}(S(2), 2^p - 1) = \text{НОД}(2^p - 1, (q-1)/2) \quad \text{и} \quad \text{НОД}\left(S(2), \frac{2^{pq}-1}{(2^p-1)(2^q-1)}\right) = 1.$$

Пусть d_2 делит $\text{НОД}(S(2), 2^q - 1)$. Тогда $(p-1) \left(T_2^{(4)}(2^{bp}) + T_3^{(4)}(2^{bp}) \right) \equiv 1 \pmod{d_2}$, и согласно соотношению (8) справедливо

$$p \equiv (p-1)^2 \left((q-1)/4 + y(T_0^{(2)}(2^u) - T_1^{(2)}(2^u))/2 \right) \pmod{d_2}$$

или в силу сравнения (4)

$$(p-1)^4 y^2 q/4 \equiv ((p-1)^2 (q-1)/4 - p)^2 \pmod{d_2}.$$

Следовательно, $d_2 < p^4 q^2$, что завершает доказательство теоремы 4. $\square$

3.3. Последовательности шестого порядка. Исследуем теперь 2-адическую сложность обобщенных циклотомических последовательностей шестого порядка. Пусть $d = 6$. Тогда $q \equiv 1 \pmod{6}$, и $4q$ можно представить следующим образом: $4q = L^2 + 27M^2$, $L \equiv 1 \pmod{3}$, $L, M \in \mathbb{Z}$ [18].

Пусть $U_0(x) = T_0^{(6)}(x) + T_1^{(6)}(x) + T_2^{(6)}(x)$ и $U_1(x) = T_3^{(6)}(x) + T_4^{(6)}(x) + T_5^{(6)}(x)$. Следующие два утверждения доказаны в [20].

Лемма 6. Пусть $4p = L^2 + 27M^2$, $L \equiv 1 \pmod{3}$ и $Z_j(c) = T_{j+2}^{(3)}(c) - T_j^{(3)}(c)$ для $j = 0, 1, 2$, $c \in \mathbb{Z}$. Тогда $Z_0(c)$, $Z_1(c)$ и $Z_2(c)$ удовлетворяют сравнению

$$X^3 - qX - qM \equiv 0 \pmod{(c^q - 1)/(c - 1)}.$$

Лемма 7. Пусть $4q = L^2 + 27M^2$, $L \equiv 1 \pmod{3}$ и $c \in \mathbb{Z}$. Тогда

A. $U_0(c)U_1(c) \equiv MZ_j(c) + (q + 1)/4 \pmod{(c^q - 1)/(c - 1)}$, когда $q \equiv 7 \pmod{12}$. Здесь $j \equiv -\text{ind}_q 2 \pmod{3}$;

B. $U_0^2(c) + U_0(c) \equiv MZ_j(c) + (q - 1)/4 \pmod{(c^q - 1)/(c - 1)}$, если $q \equiv 1 \pmod{12}$.

Теорема 5. Пусть последовательность s с периодом pq определена по формуле (1). Тогда $\Phi_2(s) \geq pq - \log_2 p - 4 \log_2 q$, если $C = Q$, и $\Phi_2(s) \geq pq - 7 \log_2 p - 4 \log_2 q$, если $C = P$.

Доказательство. Применив лемму 5 для $C = Q$, как и ранее, получим, что

$$\begin{aligned} \text{НОД}(S(2), 2^p - 1) &= \text{НОД}(2^p - 1, (q + 1)/2), \\ d_2 &= \text{НОД}(S(2), 2^q - 1) \text{ делит } (p - 1)U_1(2^{bp}) \equiv p - 1 \pmod{d_2}, \\ d_3 &= \text{НОД}\left(S(2), \frac{2^{pq} - 1}{(2^p - 1)(2^q - 1)}\right) \text{ делит } U_1(2^{bp}) + 1. \end{aligned}$$

Если r делит $U_1(2^{bp}) + 1$, то по лемме 7 $MZ_j(c) + (q \pm 1)/4 \equiv 0 \pmod{r}$ и согласно лемме 6

$$-(q \pm 1)^3/64 + M^2q(q \pm 1)/4 - qM^4 \equiv 0 \pmod{r}.$$

Значит, $d_2d_3 < (p - 1)q^3$. Применив формулу (2), получим утверждение теоремы 5 для $C = Q$. Когда $C = P$, неравенство для 2-адической сложности может быть доказано аналогично. $\square$

Заключение

Рассмотрен метод анализа 2-адической сложности обобщенных циклотомических последовательностей с периодом pq . Получены её оценки для обобщенных циклотомических последовательностей Динга–Хеллесета второго, четвертого и шестого порядков. Обобщены предыдущие результаты, полученные для последовательностей второго порядка. Применив этот же подход, можно показать, что 2-адическая сложность модернизированных последовательностей Динга–Хеллесета, предложенных в [16], больше чем $pq - 2 \log_2 p - 4 \log_2 q$, а 4-адическая сложность четвертичных последовательностей, линейная сложность которых изучена в [21], больше чем $pq - 1 - 4 \log_2 pq$.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Conflicts of Interest. The author declares no conflicts of interest.

Литература

1. *Klapper A., Goresky M.* Feedback shift registers, 2-adic span, and combiners with memory // J. Cryptol. 1997. V. 10, No 2. P. 111–147. <https://doi.org/10.1007/s001459900024>.
2. *Goresky M., Klapper A.* Algebraic Shift Register Sequences. Cambridge: Cambridge Univ. Press, 2012. xvi, 498 p. <https://doi.org/10.1017/CBO9781139057448>.
3. *Hu H.* Comments on “a new method to compute the 2-adic complexity of binary sequences” // IEEE Trans. Inf. Theory. 2014. V. 60, No 9. P. 5803–5804. <https://doi.org/10.1109/TIT.2014.2336843>.
4. *Sun Y., Wang O., Yan T.* The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation // Cryptogr. Commun. 2018. V. 10, No 3. P. 467–477. <https://doi.org/10.1007/s12095-017-0233-x>.
5. *Sun Y., Yan T., Chen Z.* The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude // Cryptogr. Commun. 2020. V. 12, No 4. P. 675–683. <https://doi.org/10.1007/s12095-019-00411-4>.
6. *Xiao Z., Zeng X.* 2-Adic complexity of two constructions of binary sequences with period $4N$ and optimal autocorrelation magnitude // Cryptogr. Commun. 2021. V. 13, No 5. P. 865–885. <https://doi.org/10.1007/s12095-021-00498-8>.
7. *Yan F., Ke P., Chang Z.* The symmetric 2-adic complexity of Tang–Gong interleaved sequences from Legendre sequence pair // Cryptogr. Commun. 2025. V. 17, No 1. P. 167–179. <https://doi.org/10.1007/s12095-024-00751-w>.
8. *Xiao Z., Zeng X., Ke M.* On the symmetric 2-adic complexity of periodic binary sequences // Adv. Math. Commun. 2024. V. 18, No 5. P. 1303–1314. <https://doi.org/10.3934/amc.2022088>.
9. *Hofer R., Winterhof A.* On the 2-adic complexity of the two-prime generator // IEEE Trans. Inf. Theory. 2018. V. 64, No 8. P. 5957–5960. <https://doi.org/10.1109/TIT.2018.2811507>.
10. *Xiao Z., Zeng X., Sun Z.* 2-Adic complexity of two classes of generalized cyclotomic binary sequences // Int. J. Found. Comput. Sci. 2016. V. 27, No 7. P. 879–893. <https://doi.org/10.1142/S0129054116500350>.
11. *Sun Y., Wang Q., Yan T.* A lower bound on the 2-adic complexity of the modified Jacobi sequences // Cryptogr. Commun. 2019. V. 11, No 2. P. 337–349. <https://doi.org/10.1007/s12095-018-0300-y>.
12. *Zhang L., Zhang J., Yang M., Feng K.* On the 2-adic complexity of the Ding–Helleseth–Martinsen binary sequences // IEEE Trans. Inf. Theory. 2020. V. 66, No 7. P. 4613–4620. <https://doi.org/10.1109/TIT.2020.2964171>.
13. *Yan M., Yan T., Li Y.* Computing the 2-adic complexity of two classes of Ding–Helleseth generalized cyclotomic sequences of periods of twin prime products // Cryptogr. Commun. 2021. V. 13, No 1. P. 15–26. <https://doi.org/10.1007/s12095-020-00451-1>.
14. *Yan T., Yan M., Sun Y., Sun S.* The 2-Adic Complexity of Ding–Helleseth Generalized Cyclotomic Sequences of Order 2 and Period pq // IEEE Access. 2020. V. 8. P. 140682–140687. <https://doi.org/10.1109/ACCESS.2020.3012570>.

15. Xiong H., Qu L., Li C. A new method to compute the 2-adic complexity of binary sequences // *IEEE Trans. Inf. Theory*. 2014. V. 60, No 4. P. 2399–2406. <https://doi.org/10.1109/TIT.2014.2304451>.
16. Ma J., Zhao W., Jia Y., Shen X., Jiang H. Linear complexity and trace representation of new Ding generalized cyclotomic sequences with period pq and order two // *Mathematics*. 2021. V. 9, No 18. Art. 2285. <https://doi.org/10.3390/math9182285>.
17. Ding C., Helleseeth T. New generalized cyclotomy and its applications // *Finite Fields*. 1998. V. 4, No 2. P. 140–166. <https://doi.org/10.1006/ffa.1998.0207>.
18. Айерланд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
19. Edemskiy V., Wu C. Symmetric 2-adic complexity of Ding-Helleseeth generalized cyclotomic sequences of period pq // Wu Y., Yung M. (Eds.) *Information Security and Cryptology: Inscrypt 2020*. Ser.: Lecture Notes in Computer Science. V. 12612. Cham: Springer, 2021. P. 318–327. https://doi.org/10.1007/978-3-030-71852-7_21.
20. Edemskiy V.A., Koltsova S.A. Symmetric 2-adic complexity of generalized cyclotomic sequences of order six with period p^n // *J. Phys.: Conf. Ser.* 2021. V. 2052. Art. 012009. <https://doi.org/10.1088/1742-6596/2052/1/012009>.
21. Ma J., Zhao W., Jia Y., Jiang H. New generalized cyclotomic quaternary sequences with large linear complexity and a product of two primes period // *Information*. 2021. V. 12, No 5. Art. 193. <https://doi.org/10.3390/info12050193>.

References

1. Klapper A., Goresky M. Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptol.*, 1997, vol. 10, no. 2, pp. 111–147. <https://doi.org/10.1007/s001459900024>.
2. Goresky M., Klapper A. *Algebraic Shift Register Sequences*. Cambridge, Cambridge Univ. Press, 2012. xvi, 498 p. <https://doi.org/10.1017/CBO9781139057448>.
3. Hu H. Comments on “a new method to compute the 2-adic complexity of binary sequences”. *IEEE Trans. Inf. Theory*, 2014, vol. 60, no. 9, pp. 5803–5804. <https://doi.org/10.1109/TIT.2014.2336843>.
4. Sun Y., Wang O., Yan T. The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation. *Cryptogr. Commun.*, 2018, vol. 10, no. 3, pp. 467–477. <https://doi.org/10.1007/s12095-017-0233-x>.
5. Sun Y., Yan T., Chen Z. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude. *Cryptogr. Commun.*, 2020, vol. 12, no. 4, pp. 675–683. <https://doi.org/10.1007/s12095-019-00411-4>.
6. Xiao Z., Zeng X. 2-Adic complexity of two constructions of binary sequences with period $4N$ and optimal autocorrelation magnitude. *Cryptogr. Commun.*, 2021, vol. 13, no. 5, pp. 865–885. <https://doi.org/10.1007/s12095-021-00498-8>.
7. Yan F., Ke P., Chang Z. The symmetric 2-adic complexity of Tang–Gong interleaved sequences from Legendre sequence pair. *Cryptogr. Commun.*, 2025, vol. 17, no. 1, pp. 167–179. <https://doi.org/10.1007/s12095-024-00751-w>.

8. Xiao Z., Zeng X., Ke M. On the symmetric 2-adic complexity of periodic binary sequences. *Adv. Math. Commun.*, 2024, vol. 18, no. 5, pp. 1303–1314. <https://doi.org/10.3934/amc.2022088>.
9. Hofer R., Winterhof A. On the 2-adic complexity of the two-prime generator. *IEEE Trans. Inf. Theory*. 2018, vol. 64, no. 8, pp. 5957–5960. <https://doi.org/10.1109/TIT.2018.2811507>.
10. Xiao Z., Zeng X., Sun Z. 2-Adic complexity of two classes of generalized cyclotomic binary sequences. *Int. J. Found. Comput. Sci.*, 2016, vol. 27, no. 7, pp. 879–893. <https://doi.org/10.1142/S0129054116500350>.
11. Sun Y., Wang Q., Yan T. A lower bound on the 2-adic comeplxity of the modified Jacobi sequences. *Cryptogr. Commun.*, 2019, vol. 11, no. 2, pp. 337–349. <https://doi.org/10.1007/s12095-018-0300-y>.
12. Zhang L., Zhang J., Yang M., Feng K. On the 2-adic complexity of the Ding–Helleseht–Martinsen binary sequences. *IEEE Trans. Inf. Theory*, 2020, vol. 66, no. 7, pp. 4613–4620. <https://doi.org/10.1109/TIT.2020.2964171>.
13. Yan M., Yan T., Li Y. Computing the 2-adic complexity of two classes of Ding–Helleseht generalized cyclotomic sequences of periods of twin prime products. *Cryptogr. Commun.*, 2021, vol. 13, no. 1, pp. 15–26. <https://doi.org/10.1007/s12095-020-00451-1>.
14. Yan T., Yan M., Sun Y., Sun S. The 2-adic complexity of Ding–Helleseht generalized cyclotomic sequences of order 2 and period pq . *IEEE Access*, 2020, vol. 8, pp. 140682–140687. <https://doi.org/10.1109/ACCESS.2020.3012570>.
15. Xiong H., Qu L., Li C. A new method to compute the 2-adic complexity of binary sequences. *IEEE Trans. Inf. Theory*, 2014, vol. 60, no. 4, pp. 2399–2406. <https://doi.org/10.1109/TIT.2014.2304451>.
16. Ma J., Zhao W., Jia Y., Shen X., Jiang H. Linear complexity and trace representation of new Ding generalized cyclotomic sequences with period pq and order two. *Mathematics*, 2021, vol. 9, no. 18, art. 2285. <https://doi.org/10.3390/math9182285>.
17. Ding C., Helleseht T. New generalized cyclotomy and its applications. *Finite Fields*, 1998, vol. 4, no. 2, pp. 140–166. <https://doi.org/10.1006/ffta.1998.0207>.
18. Ireland K., Rosen M. *Klassicheskoe vvedenie v sovremennuyu teoriyu chisel* [A Classical Introduction to Modern Number Theory]. Moscow, Mir, 1987. 416 p. (In Russian)
19. Edemskiy V., Wu C. Symmetric 2-adic complexity of Ding–Helleseht generalized cyclotomic sequences of period pq . In: Wu Y., Yung M. (Eds.) *Information Security and Cryptology: Inscrypt 2020*. Ser.: Lecture Notes in Computer Science. Vol. 12612. Cham, Springer, 2021, pp. 318–327. https://doi.org/10.1007/978-3-030-71852-7_21.
20. Edemskiy V.A., Koltsova S.A. Symmetric 2-adic complexity of generalized cyclotomic sequences of order six with period p^n . *J. Phys.: Conf. Ser.*, 2021, vol. 2052, art. 012009. <https://doi.org/10.1088/1742-6596/2052/1/012009>.
21. Ma J., Zhao W., Jia Y., Jiang H. New generalized cyclotomic quaternary sequences with large linear complexity and a product of two primes period. *Information*, 2021, vol. 12, no. 5, art. 193. <https://doi.org/10.3390/info12050193>.

Информация об авторах

Владимир Анатольевич Едемский, доктор физико-математических наук, доцент, профессор кафедры «Прикладная математика и информатика», Новгородский государственный университет им. Ярослава Мудрого

E-mail: *vladimir.edemsky@novsu.ru*

ORCID: <https://orcid.org/0000-0003-1368-3827>

Author Information

Vladimir A. Edemskiy, Doc. Sci. (Physics and Mathematics), Professor, Department of Applied Mathematics and Informatics, Yaroslav-the-Wise Novgorod State University

E-mail: *vladimir.edemsky@novsu.ru*

ORCID: <https://orcid.org/0000-0003-1368-3827>

Поступила в редакцию 16.04.2025

Принята к публикации 16.05.2025

Received April 16, 2025

Accepted May 16, 2025