

В. А. Едемский, С. А. Кольцова (Великий Новгород, НовГУ).
4-адическая сложность обобщенных циклотомических четвертичных последовательностей с четным периодом.

УДК 519.7

DOI https://doi.org/10.52513/08698325_2022_29_1_1

Резюме: Исследована 4-адическая сложность обобщенных циклотомических четвертичных последовательностей, период которых равен удвоенной степени простого числа. Рассмотренные последовательности определяются на основе классов биквадратичных вычетов. Показано, что последовательности имеют высокую 4-адическую сложность.

Ключевые слова: 4-адическая сложность, четвертичные последовательности.

Работа посвящена анализу 4-адической сложности обобщенных циклотомических четвертичных последовательностей, период которых равен удвоенной степени простого числа. В силу алгоритма рациональной аппроксимации 4-адическая сложность последовательности является важной характеристикой ее непредсказуемости. Для последовательности $s^\infty = (s_0, s_1, \dots, s_{N-1})$ над кольцом классов вычетов $\mathbb{Z}_4$ и периодом N ее 4-адическая сложность может быть определена по следующей формуле:

$$\Phi_4(s^\infty) = \log_4 \left(\frac{4^N - 1}{\text{НОД}(S(4), 4^N - 1)} \right),$$

где $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$ — порождающий многочлен последовательности.

Согласно [2], известные сбалансированные четвертичные последовательности, обладающие хорошими автокорреляционными свойствами и периодом $2p$, где p — нечетное простое число, эквивалентны последовательностям, сформированным на основе классов биквадратичных вычетов по модулю p . 4-адическая сложность таких последовательностей исследована в [1].

Метод формирования последовательностей из [2] обобщен в [3], где предложены два новых правила построения четвертичных последовательностей с периодом $2p^n$, где n — натуральное число. Рассматриваемые в [3] последовательности определяются посредством применения обобщенных циклотомических классов по модулям $2p^n$ и p^n . Показано, что эти последовательности сбалансированы и обладают высокой линейной сложностью над конечным полем четвертого порядка и кольцом четвертого порядка. Здесь распространим результаты о 4-адической сложности четвертичных последовательностей, полученные в [1], на последовательности из [3].

Пусть p — простое число такое, что $p \equiv 1 \pmod{4}$. Обозначим через g общий примитивный корень по модулям p^2 и $2p^2$. Обобщенные циклотомические классы четвертого порядка по модулям p^j и $2p^j$ для $j = 1, 2, \dots, n$ и $i = 0, \dots, 3$ определяются как:

$$D_i^{(p^j)} = \left\{ g^{i+4t} \pmod{p^j} \mid 0 \leq t < p^{j-1}(p-1)/4 \right\};$$
$$D_i^{(2p^j)} = \left\{ g^{i+4t} \pmod{2p^j} \mid 0 \leq t < p^{j-1}(p-1)/4 \right\}.$$

Тогда справедливо разбиение:

$$\mathbb{Z}_{2p^n} = \bigcup_{j=1}^n p^{n-j} \left(\bigcup_{i=0}^3 D_i^{(2p^j)} \cup 2D_i^{(p^j)} \right) \cup \{0, p^n\}.$$

Пусть

$$C_i^{(2p^n)} = \bigcup_{j=1}^n p^{n-j} D_i^{(2p^j)} \text{ и } C_i^{(p^n)} = \bigcup_{j=1}^n 2p^{n-j} D_i^{(p^j)}, \quad i = 0, 1, 2, 3$$

и $2 \bmod p \in D_e^{(p)}$.

Определим две четвертичные последовательности u^∞ и v^∞ с периодом $2p^n$ по следующим формулам:

$$u_i = \begin{cases} 0, & \text{если } i \pmod{2p^n} \in C_1^{(2p^n)} \cup C_{-e}^{(p^n)} \cup \{0\}, \\ 1, & \text{если } i \pmod{2p^n} \in C_2^{(2p^n)} \cup C_{1-e}^{(p^n)}, \\ 2, & \text{если } i \pmod{2p^n} \in C_3^{(2p^n)} \cup C_{2-e}^{(p^n)} \cup \{p^n\}, \\ 3, & \text{если } i \pmod{2p^n} \in C_0^{(2p^n)} \cup C_{3-e}^{(p^n)} \end{cases} \quad (1)$$

и

$$v_i = \begin{cases} 0, & \text{если } i \pmod{2p^n} \in C_2^{(2p^n)} \cup C_{-e}^{(p^n)} \cup \{0\}, \\ 1, & \text{если } i \pmod{2p^n} \in C_0^{(2p^n)} \cup C_{2-e}^{(p^n)}, \\ 2, & \text{если } i \pmod{2p^n} \in C_3^{(2p^n)} \cup C_{1-e}^{(p^n)} \cup \{p^n\}, \\ 3, & \text{если } i \pmod{2p^n} \in C_1^{(2p^n)} \cup C_{3-e}^{(p^n)}. \end{cases} \quad (2)$$

Согласно [3], эти последовательности обладают высокой линейной сложностью над $\mathbb{F}_4$ и $\mathbb{Z}_4$.

Теорема. Пусть s^∞ — четвертичная последовательность с периодом $2p^n$, определенная по формуле (1) или (2) для $n > 1$. Тогда для ее 4-адической сложности имеет место следующая оценка: $\Phi_4(s^\infty) \geq 2p^n - 2p^{n-1}$. Таким образом, рассмотренные последовательности имеют высокую 4-адическую сложность.

Исследование выполнено за счет гранта Российского научного фонда № 22-21-00516, <https://rscf.ru/project/22-21-00516/>

СПИСОК ЛИТЕРАТУРЫ

1. Edemskiy V., Koltsova S. Estimate of 4-adic complexity of unified quaternary sequences of length $2p$. — Adv. Math. Commun., 2022, doi: 10.3934/amc.2022048
2. Ke P., Qiao P., Yang Y. On the equivalence of several classes of quaternary sequences with optimal autocorrelation and length $2p$. — Adv. Math. Commun., 2022, v. 16, p. 285—302.
3. Ke P., Zhong Y., Zhang S. Linear complexity of a new class of quaternary generalized cyclotomic sequence with period $2p^m$. — Complexity, 2020, v. 4, p. 1–7.

UDC 519.7

DOI <https://doi.org/10.52513/08698325.2022.29.1.1>

Edemskiy V. A., Koltsova S. A. (Veliky Novgorod, Yaroslav-the-Wise Novgorod State University). **4-adic complexity of generalized cyclotomic quaternary sequences with even period.**

Abstract: The 4-adic complexity of generalized cyclotomic quaternary sequences with a period equal to twice the power of a prime is studied. These sequences based of biquadratic residue classes. It is shown that they have high 4-adic complexity.

Keywords: 4-adic complexity, quaternary sequences.