ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 30 МАТЕМАТИКИ Выпуск 1
2023

С. А. Кольцова, **В. А. Едемский** (Великий Новгород, НовГУ)**. Симметричная 2-адическая сложность бинарных последовательностей с периодом** $4N$ **.**

УДК 519.7 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Резюме: В данной работе исследована симметричная 2-адическая сложность семейства бинарных последовательностей, период которых равен $4N$. Рассмотренные последовательности получаются из пары последовательностей с идеальной автокорреляцией, имеют высокую линейную сложность и хорошие автокорреляционные свойства. Показано, что они имеют высокую симметричную 2-адическую сложность и способны противостоять алгоритму рациональной аппроксимации.

Ключевые слова: Симметричная 2-адическая сложность, бинарные последовательности.

Бинарные последовательности представляют собой интерес для многих криптографических приложений. 2-адическая и симметричная 2-адическая сложности являются важными характеристиками последовательностей. Симметричная 2-адическая сложность изучена в меньшей степени, поэтому её дальнейшее исследование является актуальным. Здесь исследуем симметричную 2-адическую сложность последовательностей, предложенных в [4].

Пусть N — нечетное натуральное число и $s = (s(0), s(1), \dots, s(N-1))$ — двоичная последовательность с периодом N. Определим две новые последовательности s_1 и s_2 с периодом N следующим образом:

$$s_1 = (s(0), s(2), \dots, s(2t), \dots) \text{ и } s_2 = (s(1), s(3), \dots, s(2t+1), \dots),$$

где $2t$ и $2t+1$ вычисляются по модулю N для $t = 0, 1, 2, \dots, N-1$.

Пусть последовательность a периода $4N$ определена как в [4]:

$$a = I(s_1, L^d(\overline{s_1}), s_2, L^d(\overline{s_2})), \tag{1}$$

где I — оператор чередования, L — оператор циклического сдвига на единицу влево, а $d \neq (N+1)/4$ — натуральное число, $\overline{s_i}$ — дополнение последовательности s_i. Эта последовательность имеет высокую линейную сложность и хорошие автокорреляционные свойства, когда s — последовательность с идеальной автокорреляцией.

2-адическая сложность последовательности определяется как наименьшая длина регистра сдвига с обратной связью по переносу, способного генерировать данную последовательность. Согласно [3], для 2-адической сложности последовательности справедливо соотношение:

$$\Phi_2(a) = \log_2\left(\frac{2^{4N}-1}{\text{НОД}\left(S_a(2), 2^{4N}-1\right)} + 1\right),$$

где $S_a(x)$ — многочлен последовательности. 2-адическая сложность последовательности a изучена в [1]. В [2] показано, что для оценки непредсказуемости последовательности предпочтительнее симметричая 2-адическая сложность, которая определяется как $\overline{\Phi_2}(a) = \min(\Phi_2(a), \Phi_2(\widetilde{a}))$. Здесь $\widetilde{a}$ — последовательность, обратная к a.

© Редакция журнала «ОПиПМ», 2023 г.

Лемма. *Пусть a — бинарная последовательность с периодом $4N$, определенная по формуле* (1). *Тогда*

$$\widetilde{a} = I(L^{N-d}(\widetilde{\overline{s_2}}), \widetilde{s_2}, L^{N-d}(\widetilde{\overline{s_1}}), \widetilde{s_1}),$$

где $\overline{s_i}$ — дополнение последовательности s_i. Воспользовавшись леммой и методом, предложенным в [1], получаем следующую теорему.

Теорема. *Пусть s — бинарная последовательность с идеальной автокорреляцией и a — последовательность с периодом $4N$, определенная по формуле* (1). *Тогда $\overline{\Phi_2}(a) = 2N + 1 - r$, где $r = НОД(4d - 1, N)$.*

Таким образом, исследованные бинарные последовательности имеют высокую симметричную 2-адическую сложность, когда НОД $(4d - 1, N) = 1$.

Исследование выполнено за счет гранта Российского научного фонда № 23–22-00516.

СПИСОК ЛИТЕРАТУРЫ

1. *Кольцова С.А., Едемский В.А.* Анализ 2-адической сложности двух семейств бинарных последовательностей. — Математические методы в технологиях и технике, 2023, № 4, с. 68–71.
2. *Hu H., Feng D.* On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences. — IEEE Trans. Inf. Theory. 2008, v. 54, p. 874–883.
3. *Klapper A., Goresky M.* Feedback shift registers, 2-adic span, and combiners with memory. — Journal of Cryptology, 1997, v. 10, p. 111–14.
4. *Meng R., Yan T.* New Constructions of two binary interleaved sequences with low autocorrelation. — International Journal of Network Security, 2017. v. 19, No. 4, p. 546-560.

UDC 519.25 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Koltsova S. A., ***Edemskiy V. A.*** (Veliky Novgorod, Yaroslav-the-Wise Novgorod State University). **Symmetric 2-adic complexity of binary sequences with a period of 4N.**

Abstract: In this paper, we study the symmetric 2-adic complexity of a family of binary sequences whose period is $4N$. The considered sequences are obtained from a pair of sequences with ideal autocorrelation, have high linear complexity and good autocorrelation properties. It is shown that they have a high symmetric 2-adic complexity and are able to resist the rational approximation algorithm.

Keywords: symmetric 2-adic complexity, binary sequences.