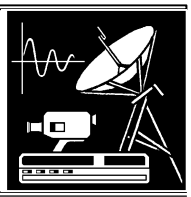
РАДИОТЕХНИКА И СВЯЗЬ



УДК 519.7 DOI: https://doi.org/10.34680/2076-8052.2021.2(123).47-51

СИММЕТРИЧНАЯ 2-АДИЧЕСКАЯ СЛОЖНОСТЬ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ 4Q И ОПТИМАЛЬНОЙ АВТОКОРРЕЛЯЦИОННОЙ МАГНИТУДОЙ

В.А.Едемский, А.В.Иванов

SYMMETRIC 2-ADIC COMPLEXITY OF BINARY SEQUENCES WITH PERIOD 4Q AND OPTIMAL AUTOCORRELATION MAGNITUDE

V.A.Edemskiy, A.V.Ivanov

Новгородский государственный университет имени Ярослава Мудрого, Vladimir.Edemsky@novsu.ru

Рассмотрены бинарные последовательности с периодом 4q, где q — нечетное простое число, и оптимальной автокорреляционной магнитудой. Последовательности определяются с использованием классов биквадратичных вычетов по простому модулю и прямого произведения колец классов вычетов. Показано, что они имеют высокую симметричную 2-адическую сложность, определяемую как наименьшее число ячеек регистра сдвига с обратной связью по переносу, который может генерировать последовательность. Симметричная 2-адическая сложность предпочтительнее 2-адической сложности при оценке непредсказуемости бинарных последовательностей. Метод исследования основан на применении обобщенных гауссовых сумм над кольцами классов вычетов. Бинарные последовательности, обладающие высокой линейной и 2-адической сложностью, хорошими автокорреляционными свойствами, представляют интерес для криптографических приложений, в частности при поточном шифровании.

Ключевые слова: бинарные последовательности, симметричная 2-адическая сложность, биквадратичные вычеты

Для цитирования: Едемский В.А., Иванов А.В. Симметричная 2-адическая сложность бинарных последовательностей с периодом 4q и оптимальной автокорреляционной магнитудой // Вестник НовГУ. Сер.: Технические науки. 2021. №2(123). С.47-51. DOI: https://doi.org/10.34680/2076-8052.2021.2(123).47-51

Binary sequences with a period of 4q (where q is an odd prime) and an optimal autocorrelation magnitude are considered. Sequences are defined using prime modulus biquadratic residue classes and direct product of residue class rings. It is shown that they have a high symmetric 2-adic complexity. The 2-adic complexity of a sequence is defined as the smallest number of carry-feedback shift register cells that is capable to generate a sequence. Symmetric 2-adic complexity is preferred over 2-adic complexity when evaluating the unpredictability of binary sequences. The research method is based on the application of generalized Gaussian sums over rings of residue classes. Binary sequences with high linear and 2-adic complexity and good autocorrelation properties are of interest for cryptographic applications, in particular, for stream encryption.

Keywords: binary sequences, symmetric 2-adic complexity, biquadratic residues

For citation: Edemskiy V.A., Ivanov A.V. Symmetric 2-adic complexity of binary sequences with period 4q and optimal autocorrelation magnitude // Vestnik NovSU. Issue: Engineering Sciences. 2021. №2(123). P.47-51. DOI: https://doi.org/10.34680/2076-8052.2021.2(123).47-51

Введение

Бинарные псевдослучайные последовательности широко применяются в различных областях. Автокорреляция, линейная сложность и 2-адическая сложность являются значимыми характеристиками бинарных последовательностей, важными для их применения в криптографии и связи. Бинарная последовательность длины $4N$ называется последовательностью с оптимальной автокорреляционной магнитудой, если значения ее периодической автокорреляционной функции принадлежат множеству $\{0,\pm 4\}$, когда значения аргумента не кратно периоду. Семейство бинарных последовательностей с оптимальной автокорреляционной магнитудой и периодом $4q$, где q — простое число и $q \equiv 5 (\mathrm{mod} 8)$, рассмотрено в [1]. Эти последовательности формируются на основе классов биквадратичных вычетов и прямого произведения колец классов вычетов по простому модулю q и модулю четыре.

Линейная сложность и 2-адическая сложность последовательности определяются, соответственно, как длина наименьшего линейного регистра сдвига с обратной связью и регистра сдвига с обратной связью по переносу, который может генерировать последовательность [2-4]. Понятие регистра сдвига с обратной связью по переносу предложено в [3], там же введено определение 2-адической сложности последовательности и рассмотрен алгоритм ее вычисления. В отличие от линейной сложности, которая хорошо изучена

для различного вида последовательностей, сформированных на классах степенных вычетов, 2-адическая сложность бинарных последовательностей изучена в меньшей степени. Основные публикации посвящены бинарным последовательностям с оптимальной автокорреляцией [5-9].

Согласно [1], если $z=\{z_i\}$ — бинарная последовательность с периодом N и $S(x)=\sum_{i=0}^{N-1} z_i x^i \in Z[x]$, тогда 2-адическая сложность последовательности z может быть определена как

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

где $\lfloor x\rfloor$ — наибольшее целое число, что меньше или равно x. Таким образом, исследование 2-адической сложности сводится к нахождению наибольшего общего делителя двух чисел. Далее, в [10] предложена другая мера оценки непредсказуемости бинарной последовательности, а именно симметричная 2-адическая сложность последовательности, определяемая как $\overline{\Phi}(z)=\min(\Phi(z),\Phi(\widetilde{z}))$, где последовательность $\widetilde{z}$ задается как $\widetilde{z}=(z_{N-1},z_{N-2},..,z_0)$. Согласно [10], для оценки секретности последовательности ее симметричная 2-адическая сложность предпочтительнее.

В этой статье изучим 2-адическую и симметричную 2-адическую сложность бинарных последовательностей из [1]. Часть результатов была представлена в [11]. Ранее в [12] показано, что эти последовательности обладают высокой линейной сложностью.

Определение последовательности

Напомним определение последовательностей из [1]. Пусть q — простое число, такое что $q\equiv 1(\bmod 4)$ и g — примитивный корень по модулю q. По определению положим, что $D_0=\{g^{4s} \bmod q; s=1,...,(q-1)/4\}$ и $D_n=g^n D_0, n=1,2,3$. Тогда D_0 — класс биквадратичных вычетов по модулю q, а D_n — его классы смежности в мультипликативной группе обратимых элементов кольца классов вычетов по модулю q. Классы вычетов $D_n, n=0,1,2,3$ также называются циклотомическими классами четвертого порядка по модулю q [13].

Отображение $\phi(a)=(a \bmod 4, a \bmod q)$ является изоморфизмом кольца классов вычетов Z_{4q} по модулю $4q$ и прямого произведения колец $Z_4\times Z_q$. Рассмотрим последовательность, определенную как в [1], по правилу

$$z_i=\begin{cases}1, \text{если } i \bmod q\in C,\\ 0, \text{иначе,}\end{cases} \qquad (1)$$

для $C=\phi^{-1}(\{0\}\times(D_l\cup D_m)\cup\{1\}\times(D_l\cup D_k)\cup\{2\}\times \times(D_m\cup D_n)\cup\{2\}\times(D_l\cup D_m)\cup G\times\{0\})$, где l,m,n и k попарно различные индексы между 0 и 3, $G=\{0,2\}$ или $G=\{1,3\}$. Согласно [1], последовательность z имеет период $4q$ и оптимальную автокорреляционную магнитуду при $q=x^2+4$ и $(l,m,n,k)=(0,1,2,3);(0,3,2,1);$ $(2,3,0,1);(1,0,3,2);(1.2.3.0);(2,1,0,3);(3,0,1,2);(3,2,1,0)$.

Из представления $q=x^2+4$, $x\equiv 1(\bmod 4)$ в виде суммы квадратов двух целых чисел следует, что $q\equiv 5(\bmod 8)$.

Следующее утверждение является основным результатом статьи.

Теорема 1. Пусть z — бинарная последовательность с периодом $4q$, определенная по формуле (1) для $q=x^2+4$, где $x\equiv 1(\bmod 4)$ и

$$(l,m,n,k)=(0,1,2,3);(0,3,2,1);$$
$$(2,3,0,1);(1,0,3,2);(1.2.3.0);(2,1,0,3);(3,0,1,2);(3,2,1,0).$$

Тогда ее симметричная 2-адическая сложность равна $\overline{\Phi}(z)=4q-3$ для $q>5$ и $\overline{\Phi}(z)=4q-5$ для $q=5$.

Согласно теореме 1 рассматриваемые последовательности обладают высокой симметричной 2-адической сложностью.

Для доказательства теоремы воспользуемся методом, изложенным во введении, а именно покажем, что $\overline{\Phi}(z)=\left\lfloor \log_2\left(\frac{2^{4q}-1}{5}\right)\right\rfloor$ для $q>5$ и $\overline{\Phi}(z)=\left\lfloor \log_2\left(\frac{2^{20}-1}{25}\right)\right\rfloor$ для $q=5$, что равносильно утверждению теоремы 1.

Согласно введению, для доказательства последних двух формул достаточно изучить $\text{НОД}\left(S_z(2),2^{4q}-1\right)$, $\text{НОД}\left(S_{\widetilde{z}}(2),2^{4q}-1\right)$, где $S_z(X)=\sum_{i=0}^{4q-1} z_i X^i\in Z[X]$ и $S_{\widetilde{z}}(X)=\sum_{i=0}^{4q-1}\widetilde{z}_i X^i\in Z[X]$. С этой целью рассмотрим далее обобщенные гауссовы суммы, введенные в [14].

Обобщенные гауссовы суммы и их свойства

Гауссовы суммы, определяемые как $\eta_t=\sum_{i\in D_t}\alpha^i, t=0,1,2,3$, где α — комплексный или алгебраический корень q-й степени из единицы, широко применяются при исследовании линейной сложности циклотомических и обобщенных циклотомических последовательностей, а также 2-адической сложности [12,13,9]. В [14] при исследовании 2-адической сложности бинарных последовательностей из [15] предложены обобщенные гаусовы суммы, когда рассматриваются суммы по циклотомическим классам степеней 2, а не комплексных или алгебраических корней q-й степени из единицы. В этом разделе изучим некоторые свойства обобщенных гаусовых сумм, рассмотренных ранеее в [14], только здесь будем рассматривать их над $Z_{2^{4q}-1}$ — кольцом классов вычетов по модулю 16^q-1, а не над $Z_{2^{2q}-1}$, как в [14].

Пусть $\zeta_t=\sum_{i\in D_t}16^i$, $t=0,1,2,3$. Тогда $\zeta_0+\zeta_1+\zeta_2+\zeta_3\equiv -1(\bmod(16^q-1)/15-1)$.

Лемма 2. Если $a = 0,1,2,3$ и $q \equiv 5 (\mathrm{mod}\, 8)$, то

$$\sum_{t \in \{a\} \times D_i} 2^t \equiv 2^{aq} \zeta_{j-2} (\mathrm{mod}\, 2^{4q} - 1).$$

Доказательство. Если $t = \phi^{-1}(a,b)$, тогда $t \equiv qa + (q+3)3^{-1}b (\mathrm{mod}\, 4q)$, где 3^{-1} — обратный элемент к 3 по модулю q. В самом деле, $t \equiv a (\mathrm{mod}\, 4)$ и $t \equiv b (\mathrm{mod}\, q)$ для $q \equiv 1 (\mathrm{mod}\, 4)$. Следовательно,

$$\sum_{t \in \{a\} \times D_i} 2^t \equiv 2^{aq} \sum_{b \in D_i} 2^{(q+3)3^{-1}b} (\mathrm{mod}\, 2^{4q} - 1).$$

Для любого числа $b \in D_i$ при $q \equiv 5 (\mathrm{mod}\, 8)$ существует элемент $c \in D_{i-2}$, такой, что $b \equiv 4c (\mathrm{mod}\, q)$. Тогда $(q+3)b \equiv 4(q+3)c (\mathrm{mod}\, 4q)$ и

$$\sum_{b \in D_i} 2^{(q+3)3^{-1}b} \equiv \sum_{c \in D_{i-2}} 16^{(q+3)3^{-1}c} \equiv \sum_{c \in D_{i-2}} 16^c (\mathrm{mod}\, 2^{4q} - 1).$$

Утверждение леммы следует из последнего сравнения.

Следствие 3. $\sum_{t \in \{a\} \times D_i} 2^t \equiv 2^a (q-1)/4 (\mathrm{mod}\, 5)$.

Пусть $\omega_i = \sum_{t \in D_i \cup D_{i+2}} 16^t, i = 0,1$. Тогда по определению видим, что $\omega_0 = \zeta_0 + \zeta_2$, $\omega_1 = \zeta_1 + \zeta_3$ и $\omega_0 + \omega_1 \equiv -1 (\mathrm{mod}\, (16^q - 1)/15)$.

Обозначим через χ квадратичный характер $GF(q)$ — конечного поля порядка q и определим $H = \omega_0 - \omega_1 = \sum_{i \in GF^*(q)} 16^i \chi(i)$. Тогда, как в [14], получаем следующее утверждение.

Лемма 4. $H^2 \equiv q - (16^q - 1)/15 (\mathrm{mod}\, 16^q - 1)$.

Далее, рассмотренные свойства обобщенных гауссовых сумм будут применяться при исследовании $\mathrm{НОД}\left(S_z(2), 2^{4q} - 1\right)$, $\mathrm{НОД}\left(S_{\tilde{z}}(2), 2^{4q} - 1\right)$.

Симметричная 2-адическая сложность последовательности

В этом разделе докажем теорему 1. Рассмотрим первые два случая, когда $(l,m,n,k) = (0,1,2,3)$ и $(l,m,n,k) = (1,0,3,2)$. Прежде всего, заметим, что $S_z(2) \equiv 2 + 2^q (\mathrm{mod}\, 3)$ или $S_z(2) \equiv 2^q + 2^{3q} (\mathrm{mod}\, 3)$. Следовательно, 3 не является делителем $S_z(2)$ и $S_{\tilde{z}}(2)$.

Далее, согласно следствию 3 справедливо следующее сравнение:

$$S_z(2) \equiv \sum_{i \in G} 2^i + (1 + 2^q + 2^{2q} + 2^{3q})(q-1)/2 (\mathrm{mod}\, 5).$$

Следовательно, $S_z(2) \equiv 0 (\mathrm{mod}\, 5)$, так как $2^{2q} \equiv -1 (\mathrm{mod}\, 5)$ и 5 — делитель $\mathrm{НОД}\left(16^q - 1, S_z(2)\right)$. Предположим, что 25 делит $2^{2q} + 1$, тогда $2^{4q} \equiv 1 (\mathrm{mod}\, 25)$. В этом случае $q = 5$. Аналогично, можно показать, что 5 — делитель, а 25 — не делитель $\mathrm{НОД}\left(16^q - 1, S_{\tilde{z}}(2)\right)$ для $q > 5$. Таким образом, случай $q = 5$ необходимо рассмотреть отдельно.

1. Пусть $q > 5$.

Введем вспомогательный многочлен $T_z(x) = \sum_{i=0}^{4q-1} (-1)^{z_i} X^i \in Z[X]$. Тогда, воспользовавшись соотношением из [6], получаем, что

$$-2S_z(X)T_z(X^{-1}) \equiv$$
$$\equiv 4q + \sum_{\tau=1}^{4q-1} A_z(\tau) X^\tau - T(X^{-1}) \sum_{i=0}^{4q-1} X^i (\mathrm{mod}\, X^{4q} - 1),$$

где $A_z(\tau)$ — периодическая автокорреляционная функция последовательности z.

Из последнего сравнения имеем:

$$-2S_z(2)T_z(2^{-1}) \equiv 4q + \sum_{\tau=1}^{4q-1} A_w(\tau) 2^\tau (\mathrm{mod}\, 2^{4q} - 1). \quad (2)$$

Согласно [1], для $(l,m,n,k) = (0,1,2,3)$ или $(l,m,n,k) = (1,0,3,2)$ и $q = x^2 + 4y^2$ периодическая автокорреляционная функция последовательности z определяется как:

$$A_z(\tau) = \begin{cases} -4, & \text{если } \tau \bmod 4 = 0, \tau \bmod q \neq 0 \text{ или } \tau = q, 3q, \\ -4y, & \text{если } \tau \bmod 4 = 1 \text{ или } 3 \text{ и } \tau \bmod q \in D_0 \cup D_2, \\ 0, & \text{если } \tau \bmod 4 = 2, \tau \bmod q \neq 0, \\ 4y, & \text{если } \tau \bmod 4 = 1 \text{ или } 3 \text{ и } \tau \bmod q \in D_1 \cup D_3, \\ 4, & \text{если } \tau = 2q. \end{cases} \quad (3)$$

Таким образом, по лемме 2, формулам (2) и (3) получаем, что

$$-2S_z(2)T_z(2^{-1}) \equiv 4q - 4 \cdot 2^q + 4 \cdot 2^{2q} - 4 \cdot 2^{3q} -$$
$$-4(\zeta_0 + \zeta_1 + \zeta_2 + \zeta_3) - 4y(2^q + 2^{3q})(\zeta_0 + \zeta_2) +$$
$$+ 4y(2^q + 2^{3q})(\zeta_1 + \zeta_3) (\mathrm{mod}\, 2^{4q} - 1)$$

или

$$-2S_z(2)T_z(2^{-1}) \equiv 4q - 4 \cdot 2^q + 4 \cdot 2^{2q} - 4 \cdot 2^{3q} -$$
$$-4((16^q - 1)/15) - 1) - 4y(2^q + 2^{3q})H (\mathrm{mod}\, 2^{4q} - 1). \quad (4)$$

По условию $|y| = 1$. Пусть d — простой делитель $\mathrm{НОД}\left(16^q - 1, S_z(2)\right)$. Далее, рассмотрим два случая.

a) Пусть d делит $2^q - 1$ и $d > 5$. В этом случае, согласно формуле (4), $q \equiv 2yH (\mathrm{mod}\, d)$. Следовательно, по лемме 4 имеем, что $q^2 \equiv 4q (\mathrm{mod}\, d)$ и $q \equiv 4 (\mathrm{mod}\, d)$. Последнее сравнение невозможно.

b) Пусть d делит $2^q + 1$ и $d > 5$. Здесь, согласно соотношению (4), $q + 4 \equiv 2yH (\mathrm{mod}\, d)$. Следовательно, по лемме 4 видим, что $q^2 + 8q + 16 \equiv 4q (\mathrm{mod}\, d)$ и $q^2 + 4q + 16 \equiv 0 (\mathrm{mod}\, d)$. Так как d — простое, то $d = 1 + 2jq, j \geq 1$ и

$$0 \equiv 2j(q^2 + 4q + 16) \equiv -q - 4 + 32j (\mathrm{mod}\, d).$$

Здесь число $q + 4$ — нечетное, значит $-q - 4 + 32j = (1 + 2f)(1 + 2jq)$, $j \in Z$. Тогда $f = 0$, $q = 13, j = 3$ и $d = 73$. Но 73 не делит $2^{13} + 1$ и получаем противоречие.

Далее, последовательность $\tilde{z}$ на периоде равна $z_{4q-1}, \ldots, z_1, z_0$, следовательно, $A_{\tilde{z}}(\tau) = A_z(-\tau)$. По условию, $q \equiv 5 (\mathrm{mod}\, 5)$, значит $-\tau (\mathrm{mod}\, q) \in D_{i+2}$, если

$\tau \in D_i$ и $-\tau \equiv 4-\tau (\mathrm{mod}\, 4)$. Тогда, согласно (3), $A_{\tilde{z}}(\tau)$ получается из $A_z(\tau)$ изменением знака y и утверждение, что $\mathrm{НОД}\left(16^q-1, S_{\tilde{z}}(2)\right)=5$, может быть доказано тем же самым способом.

Таким образом, для $q>5$ показали, что $\mathrm{НОД}\left(16^q-1, S_z(2)\right)=\mathrm{НОД}\left(16^q-1, S_{\tilde{z}}(2)\right)=5$, тогда

$$\Phi(z)=\Phi(\tilde{z})=\overline{\Phi}(z)=\left\lfloor \log_2\left(\frac{2^{4q}-1}{5}\right)\right\rfloor = 4q-3.$$

2. Пусть $q>5$. Тогда $N=4q=20$. По модулю пять существует два первообразных корня $g=2$ и $g=3$. В первом случае $D_0=\{1\}, D_l=\{2\}, D_2=\{4\}, D_3=\{3\}$, а во втором — $D_0=\{1\}, D_l=\{3\}, D_2=\{4\}, D_3=\{2\}$. Следовательно, при изменении g получаем другой вариант для (l,m,n,k), т. е. достаточно изучить только вариант, когда $g=2$. Также рассмотрим здесь только случай $G=\{0,2\}$, так как результаты вычислений совпадают при $G=\{0,2\}$ и $G=\{1,3\}$.

а) Пусть $(l,m,n,k)=(0,1,2,3)$. Тогда несложно убедиться, что последовательности z и $\tilde{z}$ принимают следующие значения на периоде:

$z=(1,1,1,0,0,0,0,1,0,0,1,1,1,1,1,0,1,0,0,0)$ и

$\tilde{z}=(0,0,0,1,0,1,1,1,1,1,0,0,1,0,0,0,0,1,1,1)$.

В этом случае $S_z(2)\not\equiv 0(\mathrm{mod}\, 25)$, но $S_{\tilde{z}}(2)\equiv 0(\mathrm{mod}\, 25)$. Следовательно, $\Phi(z)=\left\lfloor \log_2\left(\frac{2^{20}-1}{5}\right)\right\rfloor$, $\Phi(\tilde{z})=\left\lfloor \log_2\left(\frac{2^{20}-1}{25}\right)\right\rfloor$ и $\overline{\Phi}(z)=15$.

b) Пусть $(l,m,n,k)=(0,3,2,1)$. В этом случае

$z=(1,1,0,1,0,0,0,0,1,0,1,1,0,0,1,0,1,1,1,0)$ и

$\tilde{z}=(0,1,1,1,0,1,0,0,1,1,0,1,0,0,0,0,1,0,1,1)$.

Здесь $\Phi(z)=\left\lfloor \log_2\left(\frac{2^{20}-1}{25}\right)\right\rfloor$, $\Phi(\tilde{z})=\left\lfloor \log_2\left(\frac{2^{20}-1}{5}\right)\right\rfloor$ и $\overline{\Phi}(z)=15$.

В любом случае, для $q=5$ получаем, что $\overline{\Phi}(z)=15$.

Таким образом, теорема 1 доказана для $(l,m,n,k)=(0,1,2,3)$ и $(l,m,n,k)=(0,3,2,1)$. Согласно [1], изменение набора (l,m,n,k) приводит к изменению знака периодической автокорреляционной функции последовательности, а также к перестановке номеров классов вычетов, для которых функция принимает одни и те же значения. Следовательно, утверждение теоремы 1 для оставшихся вариантов можно получить тем же самым образом, воспользовавшись значениями периодической автокорреляционной функции последовательности z, полученными в [1].

Пример 1. Пусть $q=13$, $N=4q=52$ и $g=2$. Тогда $D_0=\{1,3,9\}$, $D_l=\{2,5,6\}$, $D_2=\{4,10,12\}$, $D_3=\{7,7,11\}$ и для $(l,m,n,k)=(0,1,2,3)$ по формуле (1) получаем, что

$z=(1,1,1,1,0,0,1,0,0,1,1,0,0,0,0,1,1,0,1,1,0,1,0,0,0,0,1,1,1,1,1,1,1,1,1,1,0,1,0,1,1,0,1,0,0,0,0,1,0,0,0,1,0,0,0,1,0,1,1,0,1,0,1,1,1,1,1,1,1,1,1,0,0,0,0,1,0,1,1,0,1,1,0,0,0,1,0,0,1,0,0,1,0,0,1,1,1,1)$ и $\tilde{z}=(0,0,0,1,0,0,0,1,0,0,0,1,0,1,1,0,1,0,1,1,1,1,1,1,1,1,1,0,0,0,0,1,0,1,1,0,1,1,0,1,0,0,0,0,1,1,0,0,0,1,1,0,0,1,0,0,1,1,1,1)$.

Расчеты показывают, что для этой последовательности $\Phi(z)=\Phi(\tilde{z})=\overline{\Phi}(z)=49$.

Заключение

Исследованы 2-адическая и симметричная 2-адическая сложность бинарных последовательностей из [1] с оптимальной автокорреляционной магнитудой и периодом $4q$, где q — нечетное простое число, сравнимое с пятью по модулю восемь. 2-адическая сложность является важной характеристикой непредсказуемости последовательностей, что важно для их приложений в криптографии. У рассмотренных последовательностей симметричная 2-адическая сложность больше половины периоды, т.е. является высокой. Исследованные последовательности обладают как высокой симметричной 2-адической сложностью, так и высокой линейной сложностью, а также хорошими автокорреляционными свойствами. Такие последовательности востребованы в различных приложениях.

1. Sun Y., Shen H. New Binary Sequences of Length 4*p* with Optimal Autocorrelation Magnitude // Ars Combinatoria (A Canadian Journal of Combinatorics). 2008. V. LXXXIX (89). P.255-262.
2. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.
3. Klapper A., Goresky M. Feedback shift registers, 2-adic span, and combiners with memory // Journal of Cryptology. 1997. V.10. P.111-147.
4. Klapper A., Goresky M. Cryptanalysis based on 2-adic rational approximation // LNCS. 1995. V.963. P.262-273.
5. Sun Y, Wang Q., Yan T. The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation // Cryptography and Communications. 2018. V.10 (3). P.467-477.
6. Sun Y., Yan T., Chen Z. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude // Cryptography and Communications. 2020. V.12. P.675-683.
7. Xiao Z., Zeng X., Sun Z. 2-Adic complexity of two classes of generalized cyclotomic binary sequences // Internationl Journal of Foundations of Comput. Sci. 2016. V.27 (7). P.879-893.
8. Xiong H., Qu L., Li C. A new method to compute the 2-adic complexity of binary sequences // IEEE Trans. Inform. Theory. 2014. V.60. P.2399-2406.
9. Xiong H., Qu L., Li C. 2-Adic complexity of binary sequences with interleaved structure // Finite Fields and Their Applications. 2015. V.33. P.14-28.
10. 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(2). P.874-883.
11. Едемский В.А., Иванов А.В. О симметричной 2-адической сложности бинарных последовательностей на основе биквадратичных вычетов // Математические методы в технике и технологиях: Тр. междунар. науч. конф. Казань. СПб.: Изд-во Политехн. ун-та. 2020. Т. 12(2). С.79-81.
12. Едемский В.А., Антонова О.В. Линейная сложность обобщённых циклотомических последовательностей с периодом $2^m p^n$ // Прикладная дискретная математика. 2012. № 3(17). С.5-12.
13. Cusick T., Ding C., Renvall A. Stream Ciphers and Number Theory. Elsevier Science, 2004. 492 p.

14. Zhang L., Zhang J., Yang M., Feng K. On the 2-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences // IEEE Trans. Inform. Theory. 2020. DOI: https://doi.org/10.1109/TIT.2020.2964171
15. Ding C., Helleseth T., Martinsen H. New families of binary sequences with optimal three-valued autocorrelation // IEEE Trans. Inf. Theory. 2001. V.47(1). P.428-433.

References

1. Sun Y., Shen H. New Binary Sequences of Length 4p with Optimal Autocorrelation Magnitude // Ars Combinatoria (A Canadian Journal of Combinatorics). 2008. V. LXXXIX (89). P.255-262.
2. Lidl R., Niederreiter H. Finite Fields. Addison-Wesley, 1983, 812 p. (Rus. ed.: Konechnye polya. Moscow, Mir Publ., 1988. 820 p).
3. Klapper A., Goresky M. Feedback shift registers, 2-adic span, and combiners with memory. Journal of Cryptology, 1997, vol.10, pp.111-147.
4. Klapper A., Goresky M. Cryptanalysis based on 2-adic rational approximation. LNCS, 1995, vol.963, pp.262-273.
5. Sun Y, Wang Q., Yan T. The exact autocorrelation distribution and 2-adic complexity of a class of binary sequences with almost optimal autocorrelation. Cryptography and Communications, 2018, vol.10 (3), pp.467-477.
6. Sun Y., Yan T., Chen Z. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude. Cryptography and Communications, 2020, vol.12, pp.675-683.
7. Xiao Z., Zeng X., Sun Z. 2-Adic complexity of two classes of generalized cyclotomic binary sequences. Internationl Journal of Foundations of Comput. Sci., 2016, vol.27 (7), pp.879-893.
8. Xiong H., Qu L., Li C. A new method to compute the 2-adic complexity of binary sequences. IEEE Trans. Inform. Theory, 2014, vol.60, pp.2399-2406.
9. Xiong H., Qu L., Li C. 2-Adic complexity of binary sequences with interleaved structure. Finite Fields and Their Applications, 2015, vol.33, pp.14-28.
10. 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, vol.54(2), pp.874-883.
11. Edemskiy V.A., Antonova O.V. On symmetric 2-adic complexity of binary sequences based on biquadratic residues. Mathematical methods in engineering and technology: Proc. of int. conf. Saint Petersburg, Publishing house of Polytechnic university, 2020, vol.12 (2), pp.79-81.
12. Lineynaya slozhnost' obobshchennykh tsiklotomicheskikh posledovatel'nostey s periodom 2mpn [Linear complexity of generalized cyclotomic sequences with period 2mpn]. Prikladnaya diskretnaya matematika, 2012, no.3(17), pp.5-12.
13. Cusick T., Ding C., Renvall A. Stream Ciphers and Number Theory. Elsevier Science, 2004. 492 p.
14. Zhang L., Zhang J., Yang M., Feng K. On the 2-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences // IEEE Trans. Inform. Theory. 2020. DOI:10.1109/TIT.2020.2964171
15. Ding C., Helleseth T., Martinsen H. New families of binary sequences with optimal three-valued autocorrelation. IEEE Trans. Inf. Theory, 2001, vol.47(1), pp.428-433.