

ЛИНЕЙНАЯ СЛОЖНОСТЬ ЧЕРЕДУЮЩИХСЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОЛУЧЕННЫХ ИЗ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ХОЛЛА ИЛИ ЛЕЖАНДРА

В.А.Едемский

THE LINEAR COMPLEXITY OF INTERLEAVED SEQUENCES OBTAINED FROM HALL AND LEGENDRE SEQUENCES

V.A.Edemskiy

Институт электронных и информационных систем НовГУ, Vladimir.Edemsky@novsu.ru

Исследованы минимальный многочлен и линейная сложность чередующихся бинарных последовательностей, обладающих оптимальной периодической автокорреляционной функцией. Рассматриваемые последовательности формируются на основе последовательностей Холла или Лежандра и Холла.

Ключевые слова: чередующиеся последовательности, минимальный многочлен, линейная сложность

We explored the minimal polynomial and the linear complexity of interleaved binary sequences with optimal periodical autocorrelation. These sequences are formed on the basis of Hall sequences and Legendre—Hall sequences.

Keywords: interleaved sequences, minimal polynomial, linear complexity

Введение

Периодическая автокорреляционная функция (ПАКФ) и линейная сложность являются важными характеристиками последовательности. Последовательности, обладающие хорошими автокорреляционными свойствами и высокой линейной сложностью, важны для криптографических приложений [1]. Пусть $a_0, a_1, \dots, a_{T-1}$ — последовательности с периодом N и матрица U порядка $N \times T$ образована размещением последовательностей a_j в ее j -х столбцах, $j=0, \dots, T-1$. Тогда чередующая последовательность u периода NT получается путем последовательного объединения строк матрицы U и обозначается $I(a_0, a_1, \dots, a_{T-1})$, где I — оператор чередования. Обозначим через L оператор циклического сдвига последовательности на единицу влево.

Пусть $a = \{a_j\}, b = \{b_j\}, j=0, 1, \dots, N-1$ — бинарные последовательности с периодом N , $N \equiv 3 \pmod{4}$, обладающие оптимальной ПАКФ, тогда последовательность

$$u = I(a, b, L^{1/2}a, L^{1/2}b + 1) \quad (1)$$

также обладает оптимальной ПАКФ [2].

В случае, когда a — последовательность Лежандра, простых чисел-близнецов или m -последовательность и $b = L^{1/4+\eta}a + 1, \eta$ — натуральное число, минимальный многочлен последовательности u и ее линейная сложность были найдены в [3]. Случай последовательностей Холла [4], обладающих оптимальной ПАКФ, а также когда a, b — последовательности различных типов, остался неисследованным. В этой статье найдем минимальный многочлен и линейную сложность последовательности u в случаях, когда a и b — последовательности Холла,

а также когда a — последовательность Лежандра, а b — Холла.

Если $u = \{u_i\}$ — последовательность с периодом $4N$, то ее минимальный полином $m(t)$ и линейную сложность (LC) можно вычислить по следующим формулам [5]:

$$\begin{aligned} m(x) &= (x^{4N} - 1) / \text{НОД}(x^{4N} - 1, s(x)), \\ LC &= 4N - \deg \text{НОД}(x^{4N} - 1, s(x)), \end{aligned} \quad (2)$$

где $s(x) = u_0 + u_1x + \dots + u_{4N-1}x^{4N-1}$.

Для последовательности u , сформированной по (1), согласно [3], имеем

$$\begin{aligned} \text{НОД}(x^{4N} - 1, s(x)) &= \\ &= \frac{x^{2N} - 1}{x^2 - 1} \text{НОД}\left(\left(\frac{x^N - 1}{x - 1}\right)^2, s_a(x^4) + xs_b(x^4)\right). \end{aligned} \quad (3)$$

Здесь $s_a(x) = a_0 + a_1x + \dots + a_{N-1}x^{N-1}$.

Пусть α — примитивный корень степени N из единицы в расширении поля $GF(2)$, тогда $x^N - 1 = \prod_{j=0}^{N-1} (x - \alpha^j)$. Следовательно, согласно (2) и (3), для вычисления минимального многочлена и линейной сложности последовательности u , сформированной по (1), достаточно определить число корней многочлена $s_a(x^4) + xs_b(x^4)$ в множестве $\{\alpha^l, l=0, 1, \dots, N-1\}$ и найти их кратность.

1. Линейная сложность чередующихся последовательностей Холла

Напомним определение последовательностей Холла и приведем необходимые в дальнейшем сведения [4]. Пусть $p = A^2 + 27 = 6R + 1$ — простое число, $A \equiv 1 \pmod{3}$ и g — первообразный корень по модулю

лю p . Обозначим через $H_k, k=0, \dots, 5$ циклотомические классы шестого порядка по модулю p , т. е. $H_k = \{g^{k+6t} \bmod p, t=0, \dots, R-1\}$. Дополнительно предположим, что $3 \in H_1$, тогда $D = H_0 \cup H_1 \cup H_3$ является разностным множеством Холла [4]. Пусть $D_i = g^i D, i=0, \dots, 5$ и a_i — характеристическая последовательность D_i , т. е.

$$a_{i,j} = \begin{cases} 1, & \text{если } j \bmod p \in D_i, \\ 0, & \text{иначе.} \end{cases} \quad (4)$$

Линейная сложность последовательностей Холла была вычислена в [6]. В частности, показано, что если $a = a_0$, то $s_a(\alpha) = s_a(\alpha^{g^j})$. Более того, если $p = A^2 + 27$, то $\text{ind}_g 2 \equiv 0 \pmod{3}$ [4], следовательно, $4 \in H_0$ и $s_a(\alpha^{4l}) = s_a(\alpha^l), l=1, \dots, p-1$. Также в [6] получено, для $p \equiv 7 \pmod{8}$ при соответствующем выборе первообразного корня α имеем:

$$s_a(\alpha^l) = \begin{cases} 1, & \text{если } l \in H_0 \cup \{0\}, \\ 0, & \text{если } l \in H_1 \cup \dots \cup H_5. \end{cases} \quad (5)$$

По определению, $s_a(\alpha^l) = \sum_{v \in H_0} \alpha^v + \sum_{v \in H_1} \alpha^v + \dots + \sum_{v \in H_5} \alpha^v$. Значения сумм $\sum_{v \in H_j} \alpha^v$ были найдены в [7]. Согласно [7], если $p = A^2 + 27$ и $p \equiv 3 \pmod{8}$, то

$$s_a(\alpha^v) = \begin{cases} 1, & \text{если } v \in H_0 \cup H_1 \cup H_3 \cup H_4, \\ \gamma + 1, & \text{если } v \in H_2, \\ \gamma, & \text{если } v \in H_5, \end{cases} \quad (6)$$

где γ — корень многочлена $x^2 + x + 1$.

Теорема 1. Если бинарные последовательности a_0, a_i определены по (4) и последовательность u сформирована по (1) для $a = a_0, b = L^n a_i$, то:

1. $LC = 4 + (p-1)/6$ и $m(x) = (x-1)^4 \prod_{l \in H_0} (x - \alpha^l)$, если $p \equiv 7 \pmod{8}, i=0, \eta = (p+1)/4$;
2. $LC = p+3$ и $m(x) = (x-1)^3 (x^p - 1)$, если $p \equiv 3 \pmod{8}, i=0, \eta = (p+1)/4$;
3. $LC = 2(p+5)/3$ и $m(x) = (x-1)^4 \prod_{l \notin H_0 \cup H_i} (x - \alpha^l)^2$, если $p \equiv 7 \pmod{8}, i=1, \dots, 5, \eta = (p+1)/4$;
4. $LC = (4p+8)/3$ и $m(x) = (x^p - 1)(x-1)^3 \prod_{l \in H_2 \cup H_5} (x - \alpha^l)$, если $p \equiv 3 \pmod{8}, i=3, \eta = (p+1)/4$;
5. $LC = (5p+7)/3$ и $m(x) = (x^p - 1)(x-1)^3 \prod_{l \in H} (x - \alpha^l)$, где $H = \{1, \dots, p-1\} \setminus (H_{i-1} \cup H_{i+2})$, если $p \equiv 3 \pmod{8}, i=1, 2, 4, 5, \eta = (p+1)/4$;
6. $LC = (p+11)/3$ и $m(x) = (x-1)^4 \prod_{l \in H_0} (x - \alpha^l)^2$ для $i=0$; $LC = 4 + 2(p-1)/3$ и $m(x) = (x-1)^4 \prod_{l \in H_0 \cup H_i} (x - \alpha^l)^2$ для $i=1, \dots, 5, p \equiv 7 \pmod{8}, \eta \neq (p+1)/4$;

7. $L = 2p+2$ и $m(x) = (x^{2p} - 1)(x^2 - 1)$, если $p \equiv 3 \pmod{8}, \eta \neq (p+1)/4$.

Доказательство. Если $b = L^n a_i$, то $s_b(x) = x^{p-\eta} s_{a_i}(x)$ [8]. Следовательно,

$$\begin{aligned} \text{НОД} \left(\frac{x^{2p} - 1}{x^2 - 1}, s_a(x^4) + x s_b(x^4) \right) &= \\ &= \text{НОД} \left(\left(\frac{x^p - 1}{x - 1} \right)^2, s_a(x^4) + x^{4p-4\eta+1} s_{a_i}(x^4) \right). \end{aligned} \quad (7)$$

Обозначим $s_a(x^4) + x^{4p-4\eta+1} s_{a_i}(x^4)$ через $v(x^4)$ и рассмотрим несколько случаев.

1. Пусть $\eta = (p+1)/4$. Тогда $v(x^4) = s_a(x^4) + x^{3p} s_{a_i}(x^4)$. Если $i=0$, то $v(x^4) = (1 + x^{3p}) s_a(x^4)$, следовательно,

$$\text{НОД} \left(\left(\frac{x^p - 1}{x - 1} \right)^2, v(x^4) \right) = \frac{x^p - 1}{x - 1} \text{НОД} \left(\frac{x^p - 1}{x - 1}, s_a(x^4) \right).$$

Пусть $p \equiv 7 \pmod{8}$, тогда по (5) имеем, что

$$\text{НОД} \left(\frac{x^p - 1}{x - 1}, s_a(x^4) \right) = \prod_{l \in H_1 \cup \dots \cup H_5} (x - \alpha^l).$$

Таким образом, $LC = 4 + (p-1)/6$ и $m(x) = (x-1)^4 \prod_{l \in H_0} (x - \alpha^l)$ по (2), (3) и (7).

Если же $p \equiv 3 \pmod{8}$, то

$$\text{НОД} \left(\frac{x^p - 1}{x - 1}, s_a(x^4) \right) = 1$$

по (6). В этом случае $LC = p+3$ и $m(x) = (x-1)^3 (x^p - 1)$ по (2), (3) и (7).

Пусть $i \neq 0$, тогда $v(\alpha^{4l}) = s_a(\alpha^{4l}) + s_{a_i}(\alpha^{4lg^i})$. Таким образом, из (5) для $p \equiv 7 \pmod{8}$ получаем, что

$$v(\alpha^{4l}) = \begin{cases} 1, & \text{если } l \in H_0 \cup H_i, \\ 0, & \text{иначе.} \end{cases}$$

Для определения кратности корней многочлена $v(x^4)$ найдем его производную $v'(x^4) = x^{3p-1} s_{a_i}(x^4)$. Следовательно, для многочлена $v(x^4)$ элемент α^{4l} является кратным корнем, если $l \notin H_0$. Таким образом, $LC = 4 + 2(p-1)/3$ и $m(x) = (x-1)^4 \prod_{l \notin H_0 \cup H_i} (x - \alpha^l)^2$.

Пусть $p \equiv 3 \pmod{8}$, тогда по (6) получаем, что $v(\alpha^{4l}) = 0, l=1, \dots, p-1$ тогда и только тогда, когда $l \in H_{i-1} \cup H_{i+2}$ (индексы циклотомических классов вычисляются по модулю 6) для $i=1, 2, 4, 5$ и $l \in H_0 \cup H_1 \cup H_3 \cup H_4$ для $i=3$. Так как $v'(x^4) = x^{3p-1} s_{a_i}(x^4)$, то в этом случае многочлен $v(x^4)$ не имеет кратных корней в множестве $\{\alpha^{4l}, l=1, \dots, p-1\}$. Следовательно, $LC = p+3 + (p-1)/3$ и

$m(x)=(x^p-1)(x-1)^3 \prod_{l \in H_2 \cup H_5} (x-\alpha^l)$ для $i=3$;
 $LC=p+3+2(p-1)/3$ и $m(x)=(x^p-1)(x-1)^3 \prod_{l \in H} (x-\alpha^l)$
 для $i=1,2,4,5$, где $H=\{1,\dots,p-1\} \setminus (H_{i-1} \cup H_{i+2})$.

2. Пусть $\eta \neq (p+1)/4$. Тогда
 $v(\alpha^{4l})=s_a(\alpha^{4l})+\alpha^{1-4\eta}s_a(\alpha^{4lg^i})$ и $\alpha^{1-4\eta} \notin \{0,1,\gamma,\gamma+1\}$. Та-
 ким образом, если $p \equiv 3 \pmod{8}$, то по (6)
 $v(\alpha^{4l}) \neq 0, l=1,\dots,p-1$. Воспользовавшись формулами
 (2) и (3) получаем, что $LC=2p+2$ и
 $m(x)=(x^{2p}-1)(x^2-1)$.

Если же $p \equiv 7 \pmod{8}$, по (5) получаем, что
 $v(\alpha^{4l})=0, l=1,\dots,p-1$ тогда и только тогда, когда
 $l \in \bigcup_{j=1}^5 H_j$ для $i=0$ и $l \in \bigcup_{j=1, j \neq i}^5 H_j$ для $i=1,\dots,5$. Так
 как $v'(x^4)=x^{4p-4\eta}s_{a_i}(x^4)$, то в этом случае все пере-
 численные корни многочлена $v(x^4)$ кратные. Таким
 образом, $LC=4+(p-1)/3$ и $m(x)=(x-1)^4 \prod_{l \in H_0} (x-\alpha^l)^2$
 для $i=0$; $LC=4+2(p-1)/3$ и $m(x)=(x-1)^4 \prod_{l \in H_0 \cup H_i} (x-\alpha^l)^2$
 для $i=1,\dots,5$.

Теорема доказана.

2. Линейная сложность чередующихся последовательностей Лежандра и Холла

Последовательность Лежандра определяется как

$$c_j = \begin{cases} -1, & \text{если } j=0, \\ \left(\frac{j}{p}\right), & \text{если } j \neq 0, \end{cases}$$

где $\left(\frac{j}{p}\right)$ — символ Лежандра [9]. Линейная слож-
 ность последовательностей Лежандра была вычисле-
 на в [10]. В частности, если c — последовательность
 Лежандра, то для $p \equiv 7 \pmod{8}$ при соответствующем
 выборе первообразного корня α имеем:

$$s_c(\alpha^v) = \begin{cases} 1, & \text{если } v \in H_0 \cup H_2 \cup H_4, \\ 0, & \text{если } v \in H_1 \cup H_3 \cup H_5, \end{cases} \quad (8)$$

и для $p \equiv 3 \pmod{8}$:

$$s_c(\alpha^v) = \begin{cases} \gamma+1, & \text{если } v \in H_0 \cup H_2 \cup H_4, \\ \gamma, & \text{если } v \in H_1 \cup H_3 \cup H_5. \end{cases} \quad (9)$$

Здесь по-прежнему H_k — циклотомические
 классы шестого порядка и γ — корень многочлена
 x^2+x+1 .

Теорема 2. Пусть c — последовательность
 Лежандра и $b=L^{\eta}a_i$, где последовательность a_i оп-
 ределена по (4). Тогда для последовательности
 $u=I(c,b,L^{1/2}c,L^{1/2}b+1)$ имеем:

1. $LC=(5p+19)/6$ и $m(x)=$
 $=(x-1)^4 \prod_{l \in H_{i-2} \cup H_{i+2}} (x-\alpha^l)^2 \prod_{l \in H_i} (x-\alpha^l)$ для $i=0,2,4$;

$LC=4(p+2)/3$ и $m(x)=(x-1)^4 \prod_{l \in H} (x-\alpha^l)^2$, где
 $H=H_i \cup H_0 \cup H_2 \cup H_4$ для $i=1,3,5$, если $p \equiv 7 \pmod{8}$,
 $\eta=(p+1)/4$;

2. $LC=2p+2$ и $m(x)=(x^{2p}-1)(x^2-1)$ при $i=1,3,5$;
 $LC=(5p+7)/3$ и $m(x)=(x^p-1)(x-1)^3 \prod_{l \in G} (x-\alpha^l)$ при
 $i=0,2,4$ для $p \equiv 3 \pmod{8}$, $\eta=(p+1)/4$. Здесь
 $G=H_0 \cup H_1 \cup H_3 \cup H_4$ для $i=0$; $G=H_1 \cup H_2 \cup H_4 \cup H_5$
 для $i=2$; $G=H_0 \cup H_2 \cup H_3 \cup H_5$ для $i=4$;

3. $LC=p+3$ и $m(x)=(x-1)^4 \prod_{l \in H_0 \cup H_2 \cup H_4} (x-\alpha^l)^2$
 для $i=0,2,4$; $L=4+4(p-1)/3$ и $m(x)=$
 $=(x-1)^4 \prod_{l \in H_0 \cup H_2 \cup H_4 \cup H_i} (x-\alpha^l)^2$ для $i=1,3,5$, если
 $p \equiv 7 \pmod{8}$, $\eta \neq (p+1)/4$;

4. $LC=2p+2$ и $m(x)=(x^{2p}-1)(x^2-1)$, если
 $p \equiv 3 \pmod{8}$, $\eta \neq (p+1)/4$.

Доказательство. Как и в теореме 1 получаем,
 что

$$\begin{aligned} & \text{НОД}\left(\frac{x^{2p}-1}{x^2-1}, s_c(x^4)+xs_b(x^4)\right)= \\ & = \text{НОД}\left(\frac{x^{2p}-1}{x^2-1}, s_c(x^4)+x^{4p-4\eta+1}s_{a_i}(x^4)\right). \end{aligned} \quad (10)$$

Обозначим $s_c(x^4)+x^{4p-4\eta+1}s_{a_i}(x^4)$ через $w(x^4)$
 и рассмотрим несколько случаев.

1. Пусть $\eta=(p+1)/4$. Тогда
 $w(x^4)=s_c(x^4)+x^{3p}s_{a_i}(x^4)$ и $w'(x^4)=x^{3p-1}s_{a_i}(x^4)$.

Пусть $p \equiv 7 \pmod{8}$, тогда по (4) и (8) имеем,
 что $w(\alpha^{4l})=0, l=1,\dots,p-1$ тогда и только тогда, когда
 $l \in H_i \cup H_1 \cup H_3 \cup H_5$ для $i=0,2,4$ и $l \in H_1 \cup H_3 \cup H_5 \setminus H_i$
 для $i=1,3,5$. Если $i=0,2,4$, то α^{4l} — кратный корень
 многочлена $w(x)$ при $l \in H_1 \cup H_3 \cup H_5$, и простой ко-
 рень при $l \in H_i$. Таким образом, $LC=4+5(p-1)/6$ и

$$m(x)=(x-1)^4 \prod_{l \in H_{i-2} \cup H_{i+2}} (x-\alpha^l)^2 \prod_{l \in H_i} (x-\alpha^l) \text{ для } i=0,2,4.$$

Если же $i=1,3,5$, то все корни вида α^{4l} кратные и
 $LC=4+4(p-1)/3$ и $m(x)=(x-1)^4 \prod_{l \in H} (x-\alpha^l)^2$, где
 $H=H_i \cup H_0 \cup H_2 \cup H_4$.

Пусть $p \equiv 3 \pmod{8}$, тогда по (5) и (9)
 $w(\alpha^{4l})=0, l=1,\dots,p-1$ тогда и только тогда, когда
 $l \in H_2 \cup H_5$ для $i=0$, $l \in H_0 \cup H_3$ для $i=2$, $l \in H_1 \cup H_4$
 для $i=4$. Таким образом, $LC=2p+2$ и
 $m(x)=(x^{2p}-1)(x^2-1)$, если $i=1,3,5$; $LC=p+3+2(p-1)/3$
 и $m(x)=(x^p-1)(x-1)^3 \prod_{l \in G} (x-\alpha^l)$, если $i=0,2,4$, где
 G определена в условии теоремы 2.

2. Пусть $\eta \neq (p+1)/4$. Тогда
 $v(\alpha^{4l})=s_c(\alpha^{4l})+\alpha^{1-4\eta}s_a(\alpha^{4lg^j})$ и $\alpha^{1-4\eta} \notin \{0,1,\gamma,\gamma+1\}$, так

как $p \neq 3$. Таким образом, если $p \equiv 3 \pmod{8}$, то по (6) и (9) $v(\alpha^l) \neq 0, l=1, \dots, p-1$. Воспользовавшись формулами (2), (3) и (10), получаем, что $LC=2p+2$ и $m(x)=(x^{2p}-1)(x^2-1)$.

Если же $p \equiv 7 \pmod{8}$, то по (10) получаем, что $v(\alpha^l)=0, l=1, \dots, p-1$ тогда и только тогда, когда $l \in H_1 \cup H_3 \cup H_5$ для $i=0, 2, 4$ и $l \in H_{i-2} \cup H_{i+2}$ для $i=1, 3, 5$. Таким образом, $LC=p+3$ и $m(x)=(x-1)^4 \prod_{l \in H_0 \cup H_2 \cup H_4} (x-\alpha^l)^2$ для $i=0, 2, 4$; $L=4+4(p-1)/3$ и $m(x)=(x-1)^4 \prod_{l \in H_0 \cup H_2 \cup H_4 \cup H_i} (x-\alpha^l)^2$ для $i=1, 3, 5$.

Теорема доказана.

Заключение

В статье определены параметры чередующихся бинарных последовательностей, сформированных из последовательностей Холла или Лежандра и Холла, обладающих оптимальной периодической автокорреляционной функцией и высокой линейной сложностью, рассчитан их минимальный многочлен.

1. Cusick T.W., Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam: Elsevier, 1998. 474 p.
2. Tang X. H., Ding C. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value // IEEE Trans. Inf. Theory. 2010. V.56. P.6398-6405.
3. Li N., Tang X.H. On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude // IEEE Trans. Inf. Theory. 2011. V.57. P.7597-7604.
4. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.
5. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.
6. Kim J.H., Song H.Y. On the linear complexity of Hall's sextic residue sequences // IEEE Trans. Inf. Theory. 2001. V.47. P.2094-2096.

7. Едемский В.А. О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010. Т.22. Вып. 1. С.74-82.
8. Wang Q., Du X.N. The linear complexity of binary sequences with optimal autocorrelation // IEEE Trans. Inf. Theory. 2010. V.56. P.6388-6397.
9. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
10. Ding C., Hellesteth T., Shan W. On the linear complexity of Legendre sequences // IEEE Trans. Inform. Theory. 1998. V.44. P.1276-1278.

References

1. Cusick T.W., Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam, Elsevier Publ., 1998. 474 p.
2. Tang X.H., Ding C. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value. IEEE Trans. Inf. Theory, 2010, vol. 56, pp. 6398–6405.
3. Li N., Tang X.H. On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude. IEEE Trans. Inf. Theory, 2011, vol. 57, pp. 7597–7604.
4. Hall M. Combinatorial Theory. Wiley, New York, 1975. 423 p. (Russ. ed.: Khol M. Kombinatorika. Moscow, Mir Publ., 1970. 423 p.)
5. Lidl R., Neid H. Finite Fields (Encyclopedia of Mathematics and Its Applications), vol. 20. Reading, MA: Addison-Wesley, 1983. 820 p. (Russ. ed.: Lidl R., Niderрайтер G. Konechnye polia. Moscow, Mir Publ., 1988. 820 p.)
6. Kim, J.H., Song, H.Y. On the linear complexity of Hall's sextic residue sequences. IEEE Trans. Inf. Theory, 2001, vol. 47, pp. 2094-2096.
7. Edemskii V.A. O lineinoi slozhnosti dvoichnykh posledovatel'nostei na osnove klassov bikvadraticnykh i sheshtichnykh vychetov [On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes]. Discret. Math. Appl., 2010, vol. 20, no. 1, pp. 75–84.
8. Wang Q., Du X.N. The linear complexity of binary sequences with optimal autocorrelation. IEEE Trans. Inf. Theory, 2010, vol. 56, pp. 6388–6397.
9. Ireland K., Rosen M.A. Classical Introduction to Modern Number Theory. Springer, Berlin, 1982. 416 p. (Russ. ed.: Aierlend K., Rouzen M. Klassicheskoe vvedenie v sovremennuiu teoriiu chisel. Moscow, Mir Publ., 1987. 416 p.)
10. Ding C., Hellesteth T., Shan W. On the linear complexity of Legendre sequences. IEEE Trans. Inform. Theory, 1998., vol.44, pp. 1276–1278.