

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/17/1

УДК 519.7

### ЛИНЕЙНАЯ СЛОЖНОСТЬ ОБОБЩЁННЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ $2^m p^n$

В. А. Едемский, О. В. Антонова

*Новгородский государственный университет, г. Великий Новгород, Россия***E-mail:** Vladimir.Edemsky@novsu.ru

Предлагается метод анализа линейной сложности обобщённых циклотомических последовательностей с периодом  $2^m p^n$ , позволяющий выделять последовательности с высокой линейной сложностью. Вычисляется линейная сложность ряда последовательностей на основе классов квадратичных и биквадратичных вычетов.

**Ключевые слова:** обобщённые циклотомические последовательности, линейная сложность.

#### Введение

Линейная сложность бинарной последовательности является важным показателем её качества и определяется как длина самого короткого линейного регистра сдвига с обратной связью, который может воссоздать последовательность, т. е. если  $X = \{x_i : i = 0, 1, \dots\}$  — последовательность с периодом  $N$  над полем  $\text{GF}(2)$ , то её линейная сложность определяется как наименьшее натуральное  $L$ , для которого существуют константы  $c_1, \dots, c_L \in \text{GF}(2)$ , такие, что  $x_i = c_1 x_{i-1} + c_2 x_{i-2} + \dots + c_L x_{i-L}$  для всех  $i$ ,  $L \leq i < N$  [1]. Последовательности, обладающие высокой линейной сложностью, важны для криптографических приложений. Известны алгоритмы определения линейной сложности последовательности, например алгоритм Берлекэмп — Мессе [1]. В то же время для ряда периодических последовательностей, сформированных на основе классов степенных вычетов, линейная сложность определяется видом периода последовательности [2].

Построение последовательностей на основе классов степенных вычетов (циклотомических классов) по модулю  $N$  является одним из широко применяемых методов выработки последовательностей. Такие последовательности называются обобщёнными циклотомическими, если  $N$  составное [2]. В настоящей работе предлагается метод анализа линейной сложности ряда обобщённых циклотомических последовательностей с периодом  $N = 2^m p^n$ , где  $p$  — нечётное простое число, а  $m, n$  — натуральные числа. Вычисляется линейная сложность последовательностей на основе классов квадратичных и биквадратичных вычетов. Приведённые примеры показывают, что разработанный метод позволяет выделять последовательности с высокой линейной сложностью. Ранее линейная сложность отдельных последовательностей на основе классов квадратичных вычетов с периодом  $2p^n$  и биквадратичных вычетов с периодом  $2p$  исследовалась в [3–6].

## 1. Основные определения

Пусть  $p$  — нечётное простое число и  $d$  — натуральный делитель  $p-1$ ,  $d \geq 2$ . Хорошо известно, что всегда существует первообразный корень  $\theta$  по модулю  $p^n$  [7]. Обозначим через  $H_0 = \{\theta^{td} \bmod p^n : t = 0, \dots, p^{n-1}(p-1)/d-1\}$  класс вычетов степени  $d$  по модулю  $p^n$ . Если  $A$  — подмножество  $\mathbb{Z}_{p^n}$ , то через  $tA$  будем обозначать множество  $tA = \{ta \bmod p^n : a \in A\}$ , где  $t \in \mathbb{Z}$ .

Пусть  $H_k = \theta^k H_0$  для  $k = 0, 1, \dots, d-1$ . Классы вычетов  $H_k$  образуют разбиение множества обратимых элементов кольца  $\mathbb{Z}_{p^n}$  и являются обобщёнными циклотомическими классами.

Положим  $C_k = \bigcup_{j=0}^{n-1} p^j H_k$ , тогда

$$\mathbb{Z}_{p^n} = \bigcup_{k=0}^{d-1} C_k \cup \{0\}. \quad (1)$$

Кольцо классов вычетов  $\mathbb{Z}_N$ ,  $N = 2^m p^n$ , изоморфно прямому произведению  $\mathbb{Z}_{2^m} \otimes \mathbb{Z}_{p^n}$  относительно изоморфизма  $\varphi(a) = (a \bmod 2^m, a \bmod p^n)$  [7]. Пусть  $H_{l,k} = \varphi^{-1}(\{l\} \otimes C_k)$  для  $l = 0, 1, \dots, 2^m - 1$ ,  $k = 0, 1, \dots, d-1$ , тогда, согласно (1), справедливо разбиение

$$\mathbb{Z}_N = \bigcup_{l=0}^{2^m-1} \bigcup_{k=0}^{d-1} H_{l,k} \cup \{0, p^n, \dots, (2^m - 1)p^n\}.$$

Цель работы заключается в исследовании линейной сложности характеристических последовательностей различных объединений классов вычетов  $H_{l,k}$ . Для каждого  $l = 0, 1, \dots, 2^m - 1$  зададим  $I_l$  — подмножества индексов, элементы которых могут принимать значения от 0 до  $d-1$ , то есть  $I_l \subset \{0, 1, \dots, d-1\}$ . Введем множество  $C = \bigcup_{l=0}^{2^m-1} \bigcup_{k \in I_l} H_{l,k} \cup \{0, 2p^n, \dots, (2^m - 2)p^n\}$  и рассмотрим последовательность  $X$ , определяемую следующим образом:

$$x_i = \begin{cases} 1, & \text{если } i \bmod N \in C, \\ 0 & \text{иначе.} \end{cases} \quad (2)$$

Так как, согласно определению,  $x_i = x_{i \bmod N}$ , то  $N$  является периодом последовательности  $X$ .

Далее рассмотрим метод вычисления линейной сложности последовательностей, определяемых формулой (2), и проиллюстрируем его на примерах.

## 2. Метод анализа линейной сложности последовательностей с периодом $2^m p^n$

Хорошо известно (см., например, [1]), что если  $S(t)$  — производящая функция цикла последовательности, то есть  $S(t) = x_0 + x_1 t + \dots + x_{N-1} t^{N-1}$ ,  $S(t) \in \text{GF}(2)[t]$ , то её минимальный многочлен  $m(t)$  и линейную сложность  $L$  можно определить по следующим формулам:

$$m(t) = (t^N - 1) / \text{НОД}(t^N - 1, S(t)), \quad L = N - \deg[\text{НОД}(t^N - 1, S(t))]. \quad (3)$$

В нашем случае, в кольце  $\text{GF}(2)[t]$ , справедливо разложение  $t^{2^m p^n} - 1 = (t^{p^n} - 1)^{2^m}$ , то есть

$$L = N - \deg[\text{НОД}((t^{p^n} - 1)^{2^m}, S(t))]. \quad (4)$$

Обозначим через  $\alpha$  примитивный корень степени  $p^n$  из единицы в расширении поля  $\text{GF}(2)$ ; тогда, согласно формулам (3) и (4), для вычисления минимального многочлена и линейной сложности последовательности  $X$  достаточно найти корни многочлена  $S(t)$  в множестве  $\{\alpha^v : v = 0, 1, \dots, p^n - 1\}$  и определить их кратность.

Согласно определению последовательности, имеем

$$S(\alpha^v) = \sum_{l=0}^{2^m-1} \sum_{k \in I_l} \sum_{u \in H_{l,k}} \alpha^{vu} + \sum_{j=0}^{2^{m-1}-1} \alpha^{jv2p^n}. \quad (5)$$

**Лемма 1.** Для любых  $l = 0, 1, \dots, 2^m - 1$  и  $k = 0, 1, \dots, d - 1$  справедливо равенство  $\sum_{u \in H_{l,k}} \alpha^u = \sum_{w \in C_k} \alpha^w$ .

**Доказательство.** По определению  $\alpha$  имеем, что  $\alpha^u = \alpha^{u \bmod p^n}$ , а так как  $\{u \bmod p^n : u \in H_{l,k}\} = C_k$ , то это и доказывает лемму 1. ■

Из леммы 1 и формулы (5) видно, что если один и тот же индекс  $k$  принадлежит двум разным подмножествам  $I_s$  и  $I_f$ , то соответствующий вклад классов вычетов  $H_{s,k}$  и  $H_{f,k}$  при вычислении значений  $S(\alpha^v)$  будет нулевой. Введём два новых подмножества индексов  $I = \{k : k = 0, 1, \dots, d - 1 \text{ и } \sum_{j=0}^{2^{m-1}-1} |\{k\} \cap I_{2j}| - \text{нечётное число}\}$  и  $J = \{k : k = 0, 1, \dots, d - 1 \text{ и } \sum_{j=0}^{2^{m-1}-1} |\{k\} \cap I_{2j+1}| - \text{нечётное число}\}$ .

Далее, метод вычисления значений производящей функции последовательности с периодом  $p^n$ , то есть сумм  $\sum_{w \in C_l} \alpha^w$ , предложен в [8]. Введём дополнительно следующие обозначения. Пусть  $\beta = \alpha^{p^{n-1}}$  — первообразный корень степени  $p$  из единицы в расширении поля  $\text{GF}(2)$  и  $S_d(t) = \sum_{u \in H_0} t^{u \bmod p}$ , то есть  $S_d(t)$  — многочлен, соответствующий классу вычетов степени  $d$  по модулю  $p$ . Тогда, согласно [8], если  $v \in p^f H_j$ , то  $\sum_{u \in C_k} \alpha^{uv} = S_d(\beta^{\theta^{j+k}}) + f(p-1)/d$ .

Отсюда, воспользовавшись леммой 1, формулой (5) и определением множеств  $I, J$ , получаем следующее утверждение (если  $I$  или  $J$  — пустое множество, то соответствующую сумму считаем равной нулю).

**Лемма 2.** Если  $v \in p^f H_j$  для  $f = 0, 1, \dots, n - 1$  и  $j = 0, 1, \dots, d - 1$ , то

$$S(\alpha^v) = \sum_{k \in I} S_d(\beta^{\theta^{j+k}}) + \sum_{k \in J} S_d(\beta^{\theta^{j+k}}) + (|I| + |J|)f(p-1)/d + \delta, \quad (6)$$

где

$$\delta = \begin{cases} 1, & \text{если } m = 1, \\ 0, & \text{если } m > 1. \end{cases}$$

Таким образом, задача вычисления значений  $S(\alpha^v)$  свелась к расчёту значений многочлена  $S_d(t)$ . Исследуем вопрос о кратных корнях многочлена  $S(t)$ .

**Лемма 3.** Если  $v \in p^f H_j$  для  $f = 0, 1, \dots, n - 1$  и  $j = 0, 1, \dots, d - 1$ , то  $\alpha^v$  — кратный корень многочлена  $S(t)$  тогда и только тогда, когда

$$\sum_{k \in I} S_d(\beta^{\theta^{j+k}}) = f|I|(p-1)/d + \delta, \quad \sum_{k \in J} S_d(\beta^{\theta^{j+k}}) = f|J|(p-1)/d.$$

**Доказательство.** Исследуем производную многочлена  $S(t)$ . Если  $u \in H_{l,k}$ , то для  $l \equiv 0 \pmod{2}$  всегда  $u \equiv 0 \pmod{2}$ , следовательно, в кольце  $\text{GF}(2)[t]$

$$\left( \sum_{u \in H_{l,k}} t^u \right)' = \begin{cases} 0, & \text{если } l - \text{чётное}, \\ \sum_{u \in H_{k,l}} t^{u-1}, & \text{если } l - \text{нечётное}. \end{cases}$$

Таким образом,  $S'(t) = \sum_{l=0}^{2^{m-1}-1} \sum_{k \in I_{2l+1}} \sum_{u \in H_{2l+1,k}} t^{u-1}$ . Тогда по формуле (6) и лемме 1 имеем

$$\begin{aligned} S'(\alpha^v) &= \alpha^{-v} \sum_{l=0}^{2^{m-1}-1} \sum_{k \in I_{2l+1}} \left( S_d(\beta^{\theta^{j+k}}) + f(p-1)/d \right) = \\ &= \alpha^{-v} \left( \sum_{k \in J} S_d(\beta^{\theta^{j+k}}) + \sum_{l=0}^{2^{m-1}-1} |I_{2l+1}| f(p-1)/d \right), \end{aligned}$$

или

$$S'(\alpha^v) = \alpha^{-v} \left( \sum_{k \in J} S_d(\beta^{\theta^{j+k}}) + |J| f(p-1)/d \right). \quad (7)$$

Таким образом, если  $\alpha^v$  — кратный корень многочлена  $S(t)$ , то  $S(\alpha^v) = S'(\alpha^v) = 0$  и утверждение леммы 3 следует из формул (7) и (8). Наоборот, если выполняется условие леммы 3, то по (7) и (8) имеем, что  $S(\alpha^v) = S'(\alpha^v) = 0$ , то есть  $\alpha^v$  — кратный корень многочлена  $S(t)$ . ■

Леммы 2 и 3 показывают, что для определения корней многочлена  $S(t)$  в множестве  $\{\alpha^v : v = 0, 1, \dots, N-1\}$  и выделения среди них кратных достаточно знать числа  $S_d(\beta^{\theta^l})$ ,  $l = 0, 1, \dots, d-1$ . При этом если  $v, u \in p^f H_j$ , то  $S(\alpha^v) = S(\alpha^u)$  и  $S'(\alpha^v) = S'(\alpha^u)$  для любых значений  $f = 0, 1, \dots, n-1$ ,  $j = 0, 1, \dots, d-1$ .

Пусть  $\mathbf{S}_d(x) = (S_d(x), S_d(x^\theta), \dots, S_d(x^{\theta^{d-1}}))$ ,  $\mathbf{R}(x) = \sum_{k \in I} \mathbf{S}_d(x^{\theta^k})$  и  $\mathbf{Q}(x) = \sum_{k \in J} \mathbf{S}_d(x^{\theta^k})$ .

Обозначим координаты вектор-функций  $\mathbf{R}(x)$  и  $\mathbf{Q}(x)$  при  $x = \beta$  через  $r_i, q_i$  для  $i = 0, 1, \dots, d-1$ .

Непосредственно из лемм 2 и 3 получаем следующее утверждение.

**Теорема 1.** Если  $v \in p^f H_j$ ,  $f = 0, 1, \dots, n-1$ ,  $j = 0, 1, \dots, d-1$ , то  $\alpha^v$  — корень многочлена  $S(t)$  тогда и только тогда, когда  $r_j + q_j = (|I| + |J|)f(p-1)/d + \delta$ , и корень  $\alpha^v$  многочлена  $S(t)$  кратный тогда и только тогда, когда  $r_j = |I|f(p-1)/d + \delta$ .

Таким образом, теорема 1 и формулы (3), (4) показывают, что известные значения  $\mathbf{R}(\beta)$ ,  $\mathbf{Q}(\beta)$ , а фактически  $\mathbf{S}_d(\beta)$ , позволяют оценить линейную сложность последовательности  $X$ . Метод вычисления значений  $\mathbf{S}_d(x)$  предложен в [9] и развит в [10], там же найдены значения  $\mathbf{S}_d(\beta^{\theta^j})$  при  $d = 2, 4, 6, 8$ . Следовательно, теорема 1 и результаты, представленные в [10], определяют метод анализа линейной сложности последовательностей с периодом  $2^m p^n$ , сформированных по правилу (2). Причём если  $m = 1$ , то можно явно рассчитать линейную сложность любой последовательности при  $d = 2, 3, 4, 6, 8$ , а если  $m > 1$  или  $d$  отлично от перечисленных, то можно подобрать такое правило построения последовательностей, при котором они заведомо будут обладать высокой линейной сложностью. Более того, вычисленные значения  $S(\alpha^v)$ ,  $v = 0, 1, \dots, p^n - 1$ , позволяют рассчитать минимальный многочлен последовательности по формуле (3).

Далее проиллюстрируем предложенный метод на примерах.

### 3. Линейная сложность последовательностей с периодом $2p^n$

Исследуем линейную сложность ряда обобщённых циклотомических последовательностей с периодом  $2p^n$ , ограничившись при этом вариантом, когда число нулей и единиц на периоде последовательности одинаково, то есть последовательности являются сбалансированными. В этом случае  $S(1) = p^n$ , то есть  $S(1) \bmod 2 = 1$ .

Не нарушая общности, всегда можно считать, что  $0 \in I_0$  и ноль является общим элементом пересечения множеств  $I_0, I_1$ , если оно непусто. Рассмотрим возможные варианты для множеств  $I_0, I_1$  при  $d = 2, 4$ . Для  $m = 1$  всегда  $I = I_0, J = I_1$ , по определению множеств  $I, J$ , и  $\delta = 1$ .

Пусть  $d = 2$ , тогда, как это показано в [3] (см. также [10]), справедливо соотношение

$$\mathbf{S}_d(\beta) = \begin{cases} (1, 0), & \text{если } p \equiv \pm 1 \pmod{8}, \\ (\mu, \mu + 1), & \text{если } p \equiv \pm 3 \pmod{8}. \end{cases} \quad (8)$$

Здесь  $\mu$  — корень уравнения  $x^2 + x + 1 = 0$  в расширении поля  $\text{GF}(2)$ .

**Лемма 4.** Если  $I_0 = I_1 = \{0\}$ , то для последовательности  $X$ , сформированной по правилу (2), линейная сложность  $L = 2p^n$ , а её минимальный многочлен  $m(t) = t^{2p^n} - 1$ .

**Доказательство.** По условию  $I = \{0\}, J = \{0\}$ , тогда  $\mathbf{R}(\beta) = \mathbf{Q}(\beta) = \mathbf{S}_2(\beta)$ . Следовательно,  $\mathbf{R}(\beta) + \mathbf{Q}(\beta) = (0, 0)$  и  $r_j + q_j = 0$  для любого  $j = 0, 1$ . А так как  $(|I| + |J|)(p - 1)/2$  — чётное число и  $\delta = 1$ , то по теореме 1  $S(\alpha^v) \neq 0$  при всех значениях  $v = 0, 1, \dots, 2p^n - 1$ . Утверждение леммы 4 следует из формул (3) и (4). ■

**Лемма 5.** Если  $I_0 = \{0\}, I_1 = \{1\}$ , то для последовательности  $X$ , сформированной по правилу (2), линейная сложность

$$L = \begin{cases} p^n + 1, & \text{если } p \equiv \pm 3 \pmod{8}, \\ (p^n + 3)/2, & \text{если } p \equiv \pm 1 \pmod{8}, \end{cases}$$

а её минимальный многочлен

$$m(t) = \begin{cases} (t^{p^n} - 1)(t - 1), & \text{если } p \equiv \pm 3 \pmod{8}, \\ (t - 1)^2 \prod_{v \in C_1} (t - \alpha^v), & \text{если } p \equiv 1 \pmod{8}, \\ (t - 1)^2 \prod_{v \in D} (t - \alpha^v), & \text{если } p \equiv -1 \pmod{8}, \end{cases}$$

где  $D = H_1 \cup pH_0 \cup \dots \cup p^{n-1}H_n \bmod 2$ .

**Доказательство.** В условиях леммы 5  $\mathbf{R}(\beta) = \mathbf{S}_2(\beta)$ , а  $\mathbf{Q}(\beta) = \mathbf{S}_2(\beta^\theta)$ , следовательно,  $\mathbf{R}(\beta) + \mathbf{Q}(\beta) = (1, 1)$  и  $r_j + q_j = 1$  для  $j = 0, 1$ . А так как  $(|I| + |J|)(p - 1)/2$  — четное число и  $\delta = 1$ , то по теореме 1  $S(\alpha^v) = 0$  при всех значениях  $v \in C_0 \cup C_1$ , то есть при  $v = 1, \dots, p^n - 1$ .

Далее, если  $v \in p^f H_j$  и  $\alpha^v$  — корень многочлена  $S(x)$ , то по теореме 1 он кратный корень, если  $r_j = f(p - 1)/2 + 1$ .

Таким образом, если  $p \equiv \pm 3 \pmod{8}$ , то по формуле (9)  $\alpha^v$  для  $v = 1, \dots, p^n - 1$  не является кратным корнем многочлена  $S(t)$  и  $L = 2p^n - (p^n - 1) = p^n + 1$ , а  $m(t) = (t^{2p^n} - 1)/((t^{p^n} - 1)(t - 1)) = (t^{p^n} - 1)(t - 1)$ .

Пусть  $p \equiv \pm 1 \pmod{8}$ , тогда  $\mathbf{R}(\beta) = (1, 0)$  по формуле (9). Если  $p \equiv 1 \pmod{8}$ , то  $f(p - 1)/2 + \delta \equiv 1 \pmod{2}$ , то есть  $\alpha^v$  — кратный корень многочлена  $S(t)$  для любого  $v \in C_0$ . Если же  $p \equiv -1 \pmod{8}$ , то соответственно получаем, что  $\alpha^v$  — кратный корень многочлена  $S(t)$ , когда  $r_j = f + 1$ , то есть при  $v \in H_0 \cup pH_1 \cup \dots \cup p^{n-1}H_{(n-1) \bmod 2}$ .

В обоих случаях  $L = 2p^n - (p^n - 1) - (p^n - 1)/2 = (p^n + 3)/2$ , но минимальные многочлены последовательностей, вычисленные по формуле(3), различаются. ■

В частном случае, когда  $2 \in H_0$ , утверждения лемм 4 и 5 были получены в [5, 6] другим способом.

Пусть  $d = 4$ , тогда справедливо разложение  $p = x^2 + 4y^2$ , где  $x \equiv 1 \pmod{4}$ ,  $x$  и  $y$  — целые числа [7]. Обозначим через  $\left(\frac{a}{p}\right)$  символ Лежандра, а через  $\left(\frac{a}{p}\right)_4$  — символ 4-степенного вычета [7],  $\left(\frac{a}{p}\right)_4 = 1$  тогда и только тогда, когда сравнение  $z^4 \equiv a \pmod{p}$  разрешимо в целых числах. Согласно [9, 10], имеем

1) если  $\left(\frac{2}{p}\right)_4 = 1$ , то  $\mathbf{S}_4(\beta) = (1, 1, 0, 1)$  для  $x \equiv 5 \pmod{8}$  и  $\mathbf{S}_4(\beta) = (1, 0, 0, 0)$  для  $x \equiv 1 \pmod{8}$ ;

2) если  $\left(\frac{2}{p}\right)_4 = 1$  и  $\left(\frac{2}{p}\right)_4 \neq 1$ , то  $\mathbf{S}_4(\beta) = (\mu, 0, \mu + 1, 0)$  для  $x \equiv 5 \pmod{8}$  и  $\mathbf{S}_4(\beta) = (\mu, 1, \mu + 1, 1)$  для  $x \equiv 1 \pmod{8}$ , где  $\mu$  — корень уравнения  $t^2 + t + 1 = 0$  в расширении поля  $\text{GF}(2)$ ;

3) если  $\left(\frac{2}{p}\right)_4 \neq 1$ , то  $\mathbf{S}_4(\beta) = (\zeta, \zeta^2, \zeta^4, \zeta^8)$  или  $\mathbf{S}_4(\beta) = (\zeta, \zeta^8, \zeta^4, \zeta^2)$ , где  $\zeta$  удовлетворяет условию  $\zeta^8 + \zeta^4 + \zeta^2 + \zeta + 1 = 0$ .

Воспользуемся этими соотношениями для расчёта линейной сложности последовательностей, сформированных на основе классов биквадратичных вычетов.

**Лемма 6.** Если  $I_0 = \{0, 1\}$ , то для линейной сложности последовательности  $X$ , сформированной по правилу (2), справедливо следующее:

1)  $L = 2p^n$ , если  $I_1 = \{0, 1\}$ , или  $I_1 = \{0, 2\}$  и  $\left(\frac{2}{p}\right)_4 \neq 1$ , или  $I_1 = \{0, 3\}$  и  $\left(\frac{2}{p}\right)_4 \neq 1$ ;

2)  $L = (3p^n + 1)/2$ , если  $I_1 = \{0, 3\}$  и  $\left(\frac{2}{p}\right)_4 = 1$ ,  $\left(\frac{2}{p}\right)_4 \neq 1$ ;

3)  $L = (5p^n + 1)/4$ , если  $\left(\frac{2}{p}\right)_4 = 1$  и  $I_1 = \{0, 2\}$  или  $I_1 = \{0, 3\}$ .

**Доказательство.** Докажем лемму только для  $I_1 = \{0, 3\}$ , другие два варианта исследуются аналогично. Так как по условию  $|I| = |J| = 2$ , то, согласно теореме 1,  $S(\alpha^v) = 0$  при всех значениях  $v \in C_k$  тогда и только тогда, когда  $r_k + q_k = 1$  и при этом  $\alpha^v$  — кратный корень для любого  $v \in C_k$  тогда и только тогда, когда  $r_k = 1$ . Если  $I_0 = \{0, 1\}$  и  $I_1 = \{0, 3\}$ , то  $\mathbf{R}(\beta) = \mathbf{S}_4(\beta) + \mathbf{S}_4(\beta^\theta)$ , а  $\mathbf{R}(\beta) + \mathbf{Q}(\beta) = \mathbf{S}_4(\beta^\theta) + \mathbf{S}_4(\beta^{\theta^3})$ . Из приведённых выше соотношений для  $\mathbf{S}_4(\beta)$  получаем, что  $r_k + q_k \neq 1$  для  $k = 0, 1, 2, 3$  при  $\left(\frac{2}{p}\right)_4 \neq 1$ , следовательно,  $L = 2p^n$ . Когда же  $\left(\frac{2}{p}\right)_4 = 1$ , то  $\mathbf{R}(\beta) + \mathbf{Q}(\beta) = (0, 1, 0, 1)$ , кроме этого,  $r_k \neq 1$ ,  $k = 0, 1, 2, 3$ , при  $\left(\frac{2}{p}\right)_4 \neq 1$ , то есть в этом варианте нет кратных корней и  $L = 2p^n - 2|C_0| = (3p^n + 1)/2$ . В то же время если  $\left(\frac{2}{p}\right)_4 = 1$ , то  $\mathbf{R}(\beta) = (0, 1, 1, 0)$  ((1, 0, 0, 1)), тогда  $\alpha^v$  являются кратными корнями при  $v \in C_1(C_0)$  и  $L = 2p^n - 3|C_0| = (5p^n + 3)/4$ . ■

В частном случае, для  $n = 1$  и  $I_0 = \{0, 1\}$ ,  $I_1 = \{0, 2\}$ , линейная сложность последовательности  $X$  была исследована в [4].

**Лемма 7.** Если  $I_0 = \{0, 2\}$ ,  $I_1 = \{0, 3\}$ , то для линейной сложности последовательности  $X$ , сформированной по правилу (2), справедливы следующие равенства:

- 1)  $L = 2p^n$ , если  $\left(\frac{2}{p}\right) \neq 1$ ;
- 2)  $L = p^n + 1$ , если  $\left(\frac{2}{p}\right)_4 = 1$ .

Лемма 7 доказывается подобно лемме 6. Все другие варианты для  $I_0, I_1$  сводятся к уже рассмотренным.

#### 4. Примеры оценки линейной сложности последовательностей с периодом $2^m p^n$

Рассмотрим три примера оценки линейной сложности последовательности. В [10, 11] предложено несколько правил построения последовательностей с периодами  $4p, 8p$ , обладающих хорошей периодической автокорреляционной функцией. Оценим линейную сложность этих последовательностей в общем случае. Предварительно отметим, что для всех рассматриваемых последовательностей единица является корнем многочлена  $S(x)$  при  $m > 1$  и её кратность не превосходит  $m$ .

**Лемма 8.** Если  $d = 2$  и последовательность  $X$  с периодом  $4p^n$  определена правилом (2) при  $I_0 = I_1 = I_2 = \{0\}$ ,  $I_3 = \{1\}$ , то  $L \geq 4p^n - 4$ .

**Доказательство.** Согласно условию леммы и определению множеств  $I$  и  $J$ , имеем  $I = \emptyset$ ,  $J = \{0, 1\}$ , тогда  $r_j + q_j = 1$ ,  $j = 0, 1$ , так как сумма  $\sum_{i=0}^{d-1} S_d(\beta^{\theta^i}) = 1$  [10], то есть, по теореме 1,  $S(\alpha^v) = 1$  для  $v = 1, \dots, p^n - 1$ . Таким образом, утверждение леммы следует из формулы (4). ■

**Лемма 9.** Если  $d = 4$  и последовательность  $X$  с периодом  $4p^n$  определена правилом (2) при  $I_0 = I_1 = \{0, 1\}$  и  $I_2 = \{0, 3\}$ ,  $I_3 = \{1, 2\}$  или  $I_2 = \{1, 2\}$ ,  $I_3 = \{0, 3\}$ , то  $L \geq 4p^n - 4$ .

Лемма 9 доказывается аналогично лемме 8.

**Лемма 10.** Если  $d = 4$  и последовательность  $X$  с периодом  $8p^n$  определена правилом (2) при  $I_0 = I_1 = I_2 = I_5 = \{0\}$ ,  $I_3 = \{1\}$ ,  $I_4 = I_6 = \{2\}$  и  $I_7 = \{3\}$ , то  $L \geq 8p^n - 8$ , если  $\left(\frac{2}{p}\right) \neq 1$ , и  $L \geq 4p^n - 8$ , если  $\left(\frac{2}{p}\right) = 1$ .

**Доказательство.** В условиях леммы  $S(1) = 0$  и  $I = \emptyset$ ,  $J = \{1, 3\}$ , тогда  $\mathbf{R}(\beta) = \mathbf{0}$ . Если  $\left(\frac{2}{p}\right) \neq 1$ , то  $q_i \neq 1$ , следовательно, по теореме 1  $S(\alpha^v) \neq 0$  для  $v = 1, \dots, p^n - 1$ . Если же  $\left(\frac{2}{p}\right) = 1$ , то  $\mathbf{Q}(\beta) = (0, 1, 0, 1)$  и по теореме 1  $S(\alpha^v) = 0$  для  $v \in C_0 \cup C_2$ , причём каждый корень является кратным. Применение формулы (4) завершает доказательство леммы 10. ■

#### Заключение

Предложен метод анализа линейной сложности последовательностей с периодом  $2^m p^n$ , построенных на основе обобщённых циклотомических классов. Метод позволяет как явно рассчитать линейную сложность и минимальный многочлен рассматриваемых последовательностей, так и оценить её, а также определить характеристики последовательностей, обладающих заведомо высокой линейной сложностью. Вычисле-

на линейная сложность ряда последовательностей на основе классов квадратичных и биквадратичных вычетов.

#### ЛИТЕРАТУРА

1. Лидл Р., Хидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.
2. Cusick T. W., Ding C., and Renvall A. Stream Ciphers and Number Theory. North-Holland Mathematical Library. V. 55. Amsterdam: Elsevier, 1998.
3. Ding C., Helleseeth T., and Shan W. On the Linear Complexity of Legendre Sequences // IEEE Trans. Info Theory. 1998. V. IT-44. P. 1276–1278.
4. Ding C., Helleseeth T., and Martinsen H. New families of binary sequences with optimal three-level autocorrelation // IEEE Trans. Info Theory. 2001. V. 47. P. 428–433.
5. Zhang J., Zhao C.-A., and Ma X. Linear complexity of generalized cyclotomic binary sequences of length  $2p^m$  // Appl. Algebra Eng. Commun. Comput. 2010. V. 21. No. 2. P. 93–108.
6. Zhang J., Zhao C.-A., and Ma X. On the Linear Complexity of Generalized Cyclotomic Binary Sequences with Length  $2p^2$  // IEICE Trans. Fundament. Electron., Commun. Comput. Sci. 2010. V. E93.A. Iss. 1. P. 302–308.
7. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
8. Edemskiy V. A. About computation of the linear complexity of generalized cyclotomic sequences with period  $p^{n+1}$  // Designs, Codes and Cryptography. 2011. V. 61. No. 3. P. 251–260.
9. Едемский В. А. О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010. Т. 22. № 1. С. 74–82.
10. Едемский В. А., Гантмахер В. Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. Великий Новгород: НовГУ, 2009. 189 с.
11. Zhang Y., Lei J. G., and Zhang S. P. A new family of almost differences sets and some necessary conditions // IEEE Trans. Info. Theory. 2006. V. 52. P. 2052–2061.