УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2024, Т. 166, кн. 2
С. 162–172

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 519.7

doi: 10.26907/2541-7746.2024.2.162-172

О ЛИНЕЙНОЙ СЛОЖНОСТИ ОБОБЩЕННЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕЧЕТНОГО ПЕРИОДА

В.А. Едемский

*Новгородский государственный университет им. Ярослава Мудрого,
г. Великий Новгород, 173003, Россия*

Аннотация

Оценена линейная сложность новых обобщенных циклотомических последовательностей с нечетным периодом. Для определения последовательностей применены обобщенные циклотомические классы по составному модулю. Получены достаточные условия существования бинарных и небинарных последовательностей с высокой линейной сложностью. Обобщены результаты о линейной сложности, полученные ранее для последовательностей, период которых равен степени простого числа.

Ключевые слова: обобщенная циклотомическая последовательность, линейная сложность

Введение

Псевдослучайные последовательности широко применяются в различных областях и имеют множество характеристик, таких как период, сбалансированность, автокорреляция, сложность и др. Одной из важных характеристик непредсказуемости последовательности является её линейная сложность. Для синтеза последовательностей с высокой линейной сложностью применяют различные методы, в том числе основанные на использовании математического аппарата алгебры и теории чисел. Один из таких методов заключается в использовании циклотомических и обобщенных циклотомических классов для определения последовательностей [1]. Многочисленные семейства последовательностей с высокой линейной сложностью получены с использованием классической циклотомии, обобщенных циклотомий Уитмена и Динга – Хеллесета [2–4]. Новая обобщенная циклотомия была развита в [5] при поиске последовательностей скачкообразной перестройки частоты. В отличие от циклотомий, известных ранее, здесь число циклотомических классов является функцией модуля. Далее, эта новая циклотомия применена в [6] для построения бинарных последовательностей с периодом p^n, при этом была изучена линейная сложность таких последовательностей с периодом p^2. Эти результаты обобщены в [7, 8] для бинарных последовательностей с таким периодом и в [9] – для последовательностей с периодом $2p^n$. Известны также отдельные результаты для бинарных последовательностей с другими периодами (см. [10]). Таким образом, линейная сложность последовательностей на основе новых обобщенных циклотомических классов исследована не в полной мере.

В настоящей статье обобщены результаты предыдущих иссследований и получена оценка линейной сложности таких последовательностей с произвольным нечетным периодом без ограничений на число множителей в его разложении на простые числа. Результаты, полученные для бинарных последовательностей, обобщены на q-ичные последовательности.

1. Обобщенная циклотомия и новые бинарные последовательности

Напомним определение обобщенных циклотомических классов, предложенное в [5]. Применив эти классы, определим новые бинарные последовательности.

1.1. Обобщенные циклотомические классы. Пусть e – натуральное число, большее единицы, и $p_1, p_2, \ldots, p_m$ – попарно различные простые числа, такие что $p_i = 1 + f_i e,\ f_i \in \mathbb{Z}$, где $\mathbb{Z}$ – кольцо целых чисел. Определим $v = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, $k_i \geq 1,\quad i = 1, 2, \ldots, m$. Как обычно, через $\mathbb{Z}_v$ обозначим кольцо классов вычетов по модулю v, а через $\mathbb{Z}_v^*$ – группу его обратимых элементов. Тогда порядок $|\mathbb{Z}_v^*| = \varphi(v)$, где $\varphi(\cdot)$ – функция Эйлера.

Для каждого простого числа p_i существует примитивный корень g_i по модулю p_i^2, при этом g_i – также примитивный корень по модулям p_i^j для всех $j \geq 1$ [11]. Это означает, что порядок g_i по модулю p_i^j равен $\varphi(p_i^j) = p_i^{j-1}(p_i - 1)$. Далее, согласно китайской теореме об остатках существует натуральное число $g_{(v)}$, удовлетворяющее сравнениям

$$g_{(v)} \equiv g_i^{f_i p_i^{k_i - 1}} \pmod{p_i^{k_i}},\ 1 \leq i \leq m,$$

а также существуют целые числа $h_1, h_2, \ldots, h_m$ такие, что $1 \leq h_i \leq v - 1$ и

$$h_i \equiv \begin{cases} g_i \pmod{p_i^{k_i}}, \\ 1 \pmod{p_j^{k_j}}, \end{cases} \qquad 1 \leq i \neq j \leq m. \tag{1}$$

Определим $D^{(v)} = \{g_{(v)}^t \bmod v \mid t = 0, 1, \ldots, e-1\}$, тогда $D^{(v)}$ – циклическая подгруппа $\mathbb{Z}_v^*$ порядка e [5]. Зададим её классы смежности $D_I^{(v)}$ следующим образом: $\{h_1^{j_1} h_2^{j_2} \ldots h_m^{j_m} z \bmod v \mid z \in D^{(v)}\}$, где $I = (j_1, j_2, \ldots, j_m),\ 0 \leq j_i < (p_i - 1)p_i^{k_i - 1}$. Иногда $D_I^{(v)}$ называют обобщенными циклотомическими классами Zeng–Cai–Tang–Yang.

Пусть

$$\Psi^{(v)} = \{i \in \mathbb{Z}_{(p_1-1)p_1^{k_1}} \mid 0 \leq i < f_1 p_1^{k_1}\} \times \mathbb{Z}_{(p_2-1)p_2^{k_2}} \times \ldots \mathbb{Z}_{(p_m-1)p_m^{k_m}}.$$

Согласно [5] справедливы разбиения

$$\mathbb{Z}_v^* = \bigcup_{I \in \Psi^{(v)}} D_I^{(v)} \text{ и } \mathbb{Z}_v \setminus \{0\} = \bigcup_{1 \leq u,\ u \mid v} \left(\frac{v}{u} \bigcup_{I \in \Psi^{(u)}} D_I^{(u)} \right). \tag{2}$$

При определении обобщенной циклотомии в [5] использовано условие $p_1 < p_2 < \cdots < p_m$, при котором обобщенные циклотомические классы $D_I^{(v)}$ по модулю v определяются однозначно. Но в общем случае для определения классов и последовательностей, рассмотренных далее, достаточно только зафиксировать порядок множителей в разложении $v = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$. Тогда при изменении порядка множителей p_i множества $D_I^{(v)}$ также изменятся.

1.2. Определение новых бинарных последовательностей. Пусть f_i – четное число для каждого $i = 1, 2, \ldots, m$. Отметим, что все f_i заведомо будут четными, если изначально выбрать нечетное e. Определим дополнительно

$$\Psi_1^{(v)} = \{i \in \mathbb{Z}_{(p_1-1)p_1^{k_1}} \mid 0 \le i < f_1 p_1^{k_1}/2\} \times \mathbb{Z}_{(p_2-1)p_2^{k_2}} \times \ldots \mathbb{Z}_{(p_m-1)p_m^{k_m}}$$

и $\Psi_0^{(v)} = \Psi^{(v)} \setminus \Psi_1^{(v)}$. Тогда согласно определениям имеем

$$\Psi_j^{(v)} = \Psi_j^{(p_1^{(k_1)})} \times \mathbb{Z}_{(p_2-1)p_2^{k_2}} \times \ldots \mathbb{Z}_{(p_m-1)p_m^{k_m}},\ j = 0, 1. \tag{3}$$

Обозначим через $C_j^{(v)}$ объединение множеств $\bigcup_{I \in \Psi_j^{(v)}} D_I^{(v)}$, $j = 0, 1$. Применив формулу (2), получим

$$\mathbb{Z}_v^* = C_0^{(v)} \cup C_1^{(v)} \text{ и } \mathbb{Z}_v \setminus \{0\} = \bigcup_{1 \le u,\ u|v} \frac{v}{u} \left(C_0^{(u)} \cup C_1^{(u)} \right).$$

Положим $\mathcal{F}_j = \bigcup\limits_{1 \le u,\ u|v} \frac{v}{u} C_j^{(u)}$, $j = 0, 1$, и определим сбалансированную бинарную последовательность $s^\infty = (s_0, s_1, \ldots,)$ с периодом v по следующей формуле:

$$s_i = \begin{cases} 1, & \text{если } i \bmod v \in \mathcal{F}_1 \cup \{0\}, \\ 0 & \text{иначе.} \end{cases} \tag{4}$$

Здесь важно отметить, что в частном случае, когда $v = p^n$, подгруппа $D^{(v)} = \{g^{tfp^{n-1}} \mid 0 \le t < e\}$, где g – примитивный корень по модулю p^n,

$$C_1^{(v)} = \bigcup_{i=0}^{fp^{n-1}/2-1} \{g^{i+tfp^{n-1}} \mid 0 \le t < e\} \text{ и } \mathcal{F}_1 = \bigcup_{k=1}^{n} p^{n-k} C^{(p^k)}.$$

Следовательно, бинарная последовательность с периодом p^n, рассмотренная в [6], является частным случаем s^∞. Линейная сложность этих последовательностей с периодом p^2 исследована в [6]. Эти результаты обобщены в [7–10] для последовательностей с периодами $p^n, 2p^n, p^n q^m$. Таким образом, в настоящей статье продолжено исследование линейной сложности бинарных последовательностей, определяемых посредством новой обобщенной циклотомии, начатое в [6].

1.3. Линейная сложность и многочлен последовательности. Сначала напомним несколько основных фактов о линейной сложности периодических последовательностей.

Пусть $\mathbb{F}_r$ – конечное поле порядка r и s^∞ – последовательность периода v над $\mathbb{F}_r$. Тогда линейная сложность последовательности s^∞ над полем $\mathbb{F}_r$ определяется как наименьший порядок L линейного рекуррентного соотношения, которому удовлетворяют члены последовательности

$$s_{n+L} = c_{L-1} s_{n+L-1} + \ldots + c_1 s_{n+1} + c_0 s_n \quad \text{для} \quad n \ge 0,$$

где $c_0 \ne 0, c_1, \ldots, c_{L-1} \in \mathbb{F}_r$. Далее линейную сложность последовательности будем обозначать $L(s^\infty)$.

Пусть $S(x)$ – порождающий многочлен этой последовательности, то есть $S(x) = \sum_{i=0}^{v-1} s_i x^i$. Хорошо известно, что линейную сложность последовательности s^∞ можно найти по формуле

$$L(s^\infty) = v - |\{i = 0, 1, \ldots, v-1 \mid S(\alpha^i) = 0\}|, \tag{5}$$

где α – примитивный корень степени v из единицы в расширении конечного поля $\mathbb{F}_r$. Следовательно, для нахождения линейной сложности последовательности достаточно изучить корни её порождающего многочлена. С этой целью напомним несколько свойств многочлена последовательности, полученных ранее в [7] для $v = p^n$.

Пусть $T^{(p^n)}(x)$ – многочлен последовательности s^∞, когда $v = p^n$, то есть

$$T^{(p^n)}(x) = \sum_{i \in C_1^{(p^n)}} x^i + \sum_{i \in C_1^{(p^{n-1})}} x^{pi} + \cdots + \sum_{i \in C_1^{(p)}} x^{p^{n-1} i} + 1.$$

Обозначим через β примитивный корень p^n степени из единицы в алгебраическом замыкании поля $\mathbb{F}_2$. Как обычно, под $\mathbb{F}_2(\beta)$ понимаем простое расширении поля $\mathbb{F}_2$, полученное присоединением алгебраического элемента β. Свойства многочлена $T^{(p^n)}(x)$, представленные в следующей лемме, получены в [7].

Лемма 1. *Пусть $T^{(p^n)}(x)$ – многочлен последовательности s^∞, определенной по формуле (4) для $v = p^n$, $p = 1 + ef$. Тогда*

A. Если $T^{(p^n)}(\beta^a) \in \mathbb{F}_2(\beta^{p^{n-1}})$, то $a \equiv 0 \pmod{p^{n-1}}$;

B. $T^{(p^n)}(\beta^a) + T^{(p^n)}(\beta^{g^{a p^{n-1} f/2}}) = 1$ для всех $a \in \mathbb{Z}_{p^n}^*$.

2. Свойства многочлена последовательности

Докажем несколько свойств многочлена последовательности.

Пусть α – примитивный корень v-ой степени из единицы в алгебраическом замыкании $\mathbb{F}_2$. Обозначим через v_i целое число $v/p_i^{k_i}$, $i = 0, 1, \ldots, m$. По определению НОД$(v_1, \ldots, v_m) = 1$, где НОД – наибольший общий делитель чисел. Следовательно, существуют такие целые числа $a_1, a_2, \ldots, a_m$, что $a_1 v_1 + a_2 v_2 + \cdots + a_m v_m = 1$.

Пусть $\alpha_i = \alpha^{a_i v_i}$, $i = 1, 2, \ldots, m$, тогда $\alpha = \alpha_1 \alpha_2 \ldots \alpha_m$ и α_i – примитивный корень $p_i^{k_i}$-ой степени из единицы в расширении поля $\mathbb{F}_2$, так как p_i не делит a_i для всех $i = 0, 1, \ldots, m$. Значит, $\alpha_i^{p_i^{k_i - 1}}$ – примитивный корень p_i-ой степени из единицы. Обозначим через $\mathbb{K}_i$ простое расширение поля $\mathbb{F}_2$, полученное присоединением элемента $\alpha_i^{p_i^{n_i - 1}}$.

Лемма 2. *Пусть $2^{p_i - 1} \not\equiv 1 \pmod{p_i^2}$ и НОД$(p_i, p_j - 1) = 1$, $i, j = 1, 2, \ldots, m$. Тогда, если $i \neq j$, то*

$$\mathbb{F}_2(\alpha_i) \cap \mathbb{F}_2(\alpha_j) = \mathbb{K}_i \cap \mathbb{K}_j.$$

Доказательство. Ясно, что $\mathbb{K}_i \cap \mathbb{K}_j \subset \mathbb{F}_2(\alpha_i) \cap \mathbb{F}_2(\alpha_j)$. Обозначим через $[\mathbb{F}_2(\alpha_i) : \mathbb{F}_2]$ степень расширения $\mathbb{F}_2(\alpha_i)$ над $\mathbb{F}_2$. Если $2^{p_i - 1} \not\equiv 1 \pmod{p_i^2}$, то $[\mathbb{F}_2(\alpha_i) : \mathbb{F}_2] = p_i^{n_i - 1} [\mathbb{K}_i : \mathbb{F}_2]$ для каждого i : $1 \leq i \leq m$ по лемме 3 из [7]. Так как $[\mathbb{F}_2(\alpha_i) \cap \mathbb{F}_2(\alpha_j) : \mathbb{F}_2]$ делит $[\mathbb{F}_2(\alpha_i) : \mathbb{F}_2]$, $[\mathbb{F}_2(\alpha_j) : \mathbb{F}_2]$ и НОД$(p_i, p_j - 1) = 1$, то $[\mathbb{F}_2(\alpha_i) \cap \mathbb{F}_2(\alpha_j) : \mathbb{F}_2]$ делит $[\mathbb{K}_i : \mathbb{F}_2]$ и $[\mathbb{K}_j : \mathbb{F}_2]$. Последнее замечание завершает доказательство леммы. □

Отметим, что простые числа p такие, что $2^{p-1} \equiv 1 \pmod{p^2}$, встречаются редко.

Лемма 3. *Пусть $u | v$, $u = p_{j_1}^{n_1} \ldots p_{j_t}^{n_t}$ для $j_i \in \{1, 2, \ldots, m\}$, $1 \leq n_i \leq k_{j_i}, t > 1$ и $S^{(u)}(x) = \sum_{i \in C_1^{(u)}} x^{vi/u}$. Тогда $S^{(u)}(\alpha^a) \in \{0, S^{(p_{j_1}^{n_1})}(\alpha_{j_1}^{ua/v})\}$.*

Доказательство. По определению имеем $S^{(u)}(\alpha^a) = \sum_{i\in C_1^{(u)}} \alpha^{via/u}$ и $C_1^{(u)} = \bigcup_{I\in\Psi_1^{(u)}} D_I^{(u)}$. Тогда в силу формулы (3)

$$\Psi_1^{(u)} = \Psi_1^{(p_{j_1}^{(n_1)})} \times \mathbb{Z}_{(p_{j_2}-1)p_{j_2}^{n_2-1}} \times \ldots \mathbb{Z}_{(p_{j_t}-1)p_{j_t}^{n_{j_t}-1}}.$$

Пусть, как и ранее, $\alpha = \alpha_1\alpha_2\ldots\alpha_m$. Согласно сравнению (1) имеем $h_i \equiv 1 \pmod{p_j^{k_j}}$ для $j \neq i$. Следовательно, $\alpha_i^{h_1h_2\ldots h_m} = \alpha_i^{h_i}$. Значит,

$$S^{(u)}(\alpha^a) = \sum_{i\in C_1^{(p_{j_1}^{n_1})}} \alpha_{j_1}^{via/u} \cdot \sum_{i\in\mathbb{Z}^*_{p_{j_2}^{n_2}}} \alpha_{j_2}^{via/u} \cdots \sum_{i\in\mathbb{Z}^*_{p_{j_t}^{n_t}}} \alpha_{j_t}^{via/u}. \tag{6}$$

Сумма $\sum_{i\in\mathbb{Z}^*_{p_j^{n_j}}} \alpha_j^{via/u}$ равна 0 или 1 для всех значений $j, a \in \mathbb{Z}$, и

$$\sum_{i\in C_1^{(p_{j_1}^{n_1})}} \alpha_{j_1}^{via/u} = S^{(p_{j_1}^{n_1})}(\alpha_{j_1}^{ua/v}).$$

Таким образом, утверждение леммы следует из формулы (6). □

3. Линейная сложность бинарных последовательностей

Получим оценку линейной сложности рассматриваемых бинарных последовательностей. Следующее утверждение является главным результатом статьи для бинарных последовательностей.

Теорема 1. *Пусть* $2^{p_i-1} \not\equiv 1 \pmod{p_i^2}$, *НОД*$(p_i, p_j - 1) = 1$, $i, j = 1, 2, \ldots, m$, *и последовательность* s^∞ *определена по формуле* (4), *когда* $v = p_1^{k_1}p_2^{k_2}\ldots p_m^{k_m}$. *Тогда справедливы следующие оценки её линейной сложности:*

A. $L(s^\infty) \geq p_1^{k_1}p_2^{k_2}\ldots p_{m-1}^{k_{m-1}}p_m(p_m^{k_m-1} - 1)$, *если* $k_m > 1$;

B. $L(s^\infty) \geq p_1^{k_1}p_2^{k_2}\ldots p_{m-1}^{k_{m-1}}(p_m - 1)/2$, *если* $k_m = 1$.

Доказательство. Рассмотрим два случая

(i) Сначала предположим, что $k_m > 1$. Пусть

$$U_0 = \{u > 1 \mid u|v,\ u \neq p_m^j \text{ для } j = 1, 2, \ldots, k_m\}$$

и $U_1 = \{p_m, p_m^2, \ldots, p_m^{k_m}\}$. Согласно определению $\{1 \leq u,\ u|v\} = U_0 \cup U_1$. Следовательно,

$$S(\alpha^a) = 1 + \sum_{i\in\mathcal{F}_1} \alpha^{ai} = 1 + \sum_{u\in U_0} \sum_{i\in\frac{v}{u}C_1^{(u)}} \alpha^{ai} + \sum_{u\in U_1} \sum_{i\in\frac{v}{u}C_1^{(u)}} \alpha^{ai} =$$

$$= 1 + \sum_{u\in U_0} S^{(u)}(\alpha^a) + \sum_{u\in U_1} S^{(u)}(\alpha^a),$$

где $S^{(u)}(x) = \sum_{i\in C_1^{(u)}} x^{vi/u}$, как и в лемме 3.

Ясно, что

$$1 + \sum_{u\in U_1} S^{(u)}(x^i) = \sum_{i\in C_1^{(p_m^{k_m})}} x^{iv/p_m^{k_m}} + \sum_{i\in C_1^{(p_m^{k_m-1})}} x^{iv/p_m^{k_m-1}} + \cdots + \sum_{i\in C_1^{(p)}} x^{iv/p_m} + 1,$$

то есть $\sum_{u\in U_1} S^{(u)}(\alpha^a) = T^{(p_m^{k_m})}(\alpha^{av/p_m^{k_m}})$, где $T^{(p_m^{k_m})}(x)$ – многочлен последовательности, определенной по формуле (4) для $v = p_m^{k_m}$.

Пусть $S(\alpha^a) = 0$. Тогда

$$T^{(p_m^{k_m})}(\alpha^{va/p_m^{k_m}}) = 1 + \sum_{u\in U_0} S^{(u)}(\alpha^a).$$

По лемме 3

$$\sum_{u\in U_0} S^{(u)}(\alpha^a) \in \mathbb{F}_2(\alpha_1\alpha_2\dots\alpha_{m-1}) \quad \text{и} \quad T^{(p_m^{k_m})}(\alpha^{va/u}) = T^{(p_m^{k_m})}(\alpha_m^{va/p_m^{k_m}}).$$

Следовательно, согласно лемме 2 в этом случае $T^{(p_m^{n_m})}(\alpha_m^{va/p_m^{k_m}}) \in \mathbb{K}_1$. Тогда по лемме 1 имеем $a \equiv 0 \pmod{p_m^{k_m-1}}$. Так как

$$|\{a \mid a \equiv 0 \pmod{p_m^{k_m-1}},\ 0 \le a < v\}| = v/p_m^{k_m-1},$$

то

$$|\{a \mid S(\alpha^a) = 0,\ 0 \le a < v\}| \le v/p_m^{k_m-1}.$$

В результате из формулы (5) следует, что $L(s^\infty) \ge v - v/p_m^{k_m-1}$.

(ii) Пусть $k_m = 1$. Согласно китайской теореме об остатках существует такое целое число b, что $b \equiv 1 \pmod{p_i^{k_i}}$, $1 \le i \le m-1$ и $b \equiv g_m^{f_m/2} \pmod{p_m}$.

Предположим, что $S(\alpha^a) = 0$, $a \not\equiv 0 \pmod{p_m}$. Сумма $\sum_{i=1}^{p_m-1} \alpha_m^{ai}$ будет равна единице, когда $k_m = 1$. В силу лемм 1, 3 и выбора b заключаем, что справедливо равенство

$$S(\alpha^a) + S(\alpha^{ab}) = S^{(p_m)}(\alpha_m^{va/p_m}) + S^{(p_m)}(\alpha_m^{g_m^{f_m/2}va/p_m}) = 1.$$

Следовательно, хотя бы одно из этих значений не равно нулю. Далее,

$$|\{a \mid a \not\equiv 0 \pmod{p_m},\ 1 \le a \le v-1\}| = p_1^{k_1}p_2^{k_2}\dots p_{m-1}^{k_{m-1}}(p_m - 1)$$

и

$$|\{a \mid a \equiv 0 \pmod{p_m},\ 0 \le a \le v-1\}| = p_1^{k_1}p_2^{k_2}\dots p_{m-1}^{k_{m-1}}.$$

Таким образом,

$$|\{a \mid S(\alpha^a) = 0,\ 1 \le a < v\}| \le p_1^{k_1}p_2^{k_2}\dots p_{m-1}^{k_{m-1}}(p_m+1)/2$$

и $L(s^\infty) \ge p_1^{k_1}p_2^{k_2}\dots p_{m-1}^{k_{m-1}}(p_m-1)/2$. □

Отметим, что согласно теореме 1 всегда можно получить бинарную последовательность с периодом v и высокой линейной сложностью, если $k_1+k_2+\dots+k_m > m$.

4. Небинарные последовательности

Бинарные последовательности относятся к наиболее изучаемым и используемым, тем не менее исследование линейной сложности других последовательностей также представляет интерес.

Рассмотрим линейную сложность q-ичных последовательностей, определяемых на новых обобщенных циклотомических классах, когда q делит f_i для каждого значения $i = 1, 2, \dots, m$. Здесь определим

$$\Psi_j^{(v)} = \{i \in \mathbb{Z}_{(p_1-1)p_1^{k_1}} \mid jf_1p_1^{k_1}/q \le i < (j+1)f_1p_1^{k_1}/q\} \times \mathbb{Z}_{(p_2-1)p_2^{k_2}} \times \dots \mathbb{Z}_{(p_m-1)p_m^{k_m}}$$

для $j = 0, 1, \dots, q-1$.

Обозначим через $C_j^{(v)}$ множество $\bigcup_{I\in\Psi_j^{(v)}} D_I^{(v)}$, $j=0,1,\dots,q-1$. Справедливы разбиения

$$\mathbb{Z}_v^* = \bigcup_{j=0}^{q-1} C_j^{(v)} \text{ и } \mathbb{Z}_v \setminus \{0\} = \bigcup_{1<u,\ u|v} \bigcup_{j=0}^{q-1} \frac{v}{u} C_j^{(u)}.$$

Пусть $\mathcal{F}_j = \bigcup\limits_{1<u,\ u|v} \frac{v}{u} C_j^{(u)}$, $j=0,1,\dots,q-1$.

Определим сбалансированную q-ичную последовательность $u^\infty = (u_0, u_1, \dots)$ с периодом v по правилу

$$u_i = \begin{cases} 0, & \text{если } i \bmod v \in \mathcal{F}_0 \cup \{0\}, \\ j, & \text{если } i \bmod v \in \mathcal{F}_j,\ j=1,\dots,q-1. \end{cases} \tag{7}$$

Если q – простое число, то u^∞ – последовательность над конечным полем $\mathbb{F}_q$, иначе, над кольцом классов вычетов $\mathbb{Z}_q$.

Лемма 4. *Пусть q – нечетное простое число, $q^{p_i-1} \not\equiv 1 \pmod{p_i^2}$, $i = 1,2,\dots,m$, и последовательность u^∞ определена по формуле (7) для $v = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. Тогда $L(u^\infty) \ge p_1^{k_1} p_2^{k_2} \dots p_{m-1}^{k_{m-1}} (p_m-1)(q-1)/q$.*

Доказательство. Обозначим через $U(x)$ образующий многочлен последовательности u^∞ и для удобства через $U^{(p^j)}(x)$ – этот же многочлен, когда $v = p^j$. Пусть здесь α – примитивный корень v-ой степени из единицы в алгебраическом замыкании конечного поля $\mathbb{F}_q$.

Сначала рассмотрим частный случай, когда $v = p^n$. Обозначим через g примитивный корень по модулю p. Тогда

$$C_j^{(v)} = \bigcup_{i=jfp^{n-1}/q}^{(j+1)fp^{n-1}/q-1} \{g^{i+tfp^{n-1}} \mid 0 \le t < e\}$$

и $\mathcal{F}_j = \bigcup_{k=1}^n p^{n-k} C_j^{(p^k)}$, $j=0,1,\dots,q-1$. Следовательно,

$$p^{n-k} C^{(p^k)}_{(j+1) \bmod q} = g^{fp^{n-1}/q} p^{n-k} C_j^{(p^k)}.$$

Таким образом, в этом случае

$$\sum_{j=0}^{n-1} U^{(p^{n-j})}(\alpha^{ag^{fp^{n-1}/q}}) = \sum_{j=0}^{n-1} U^{(p^{n-j})}(\alpha^a) + 1$$

для $a \in \mathbb{Z}_{p^n}^*$.

Пусть $c \equiv 1 \pmod{p_i^{k_i}}$, $1 \le i \le m-1$, и $c \equiv g_m^{fp^{n-1}/q} \pmod{p_m^{k_m}}$. Тогда

$$\sum_{j=0}^{n-1} U^{(p^{n-j})}(\alpha^t) = \sum_{j=0}^{n-1} U^{(p^{n-j})}(\alpha) + t.$$

Далее, применив тот же самый метод, что и при доказательстве теоремы 1, можно показать, что и в общем случае $U(\alpha^{ac^t}) = U(\alpha^a) + t$ для $t = 1,2,\dots,q-1$. Следовательно,

$$|\{a \mid U(\alpha^a)=0,\ 1 \le a < v\}| \le |\{a \mid a \not\equiv 0 \pmod{p_m},\ 1 \le a < v\}|/q + \\ + |\{a \mid a \equiv 0 \pmod{p_m},\ 1 \le a < v\}|$$

или

$$|\{a \mid U(\alpha^a) = 0,\ 1 \le a < v\}| \le p_1^{k_1} p_2^{k_2} \dots p_m^{k_m-1}(p_m-1)/q + p_1^{k_1} p_2^{k_2} \dots p_m^{k_m-1}.$$

Окончательно получим, что

$$L(s^\infty) \ge p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} - p_1^{k_1} p_2^{k_2} \dots p_m^{k_m-1}(p_m-1)(q-1)/q.$$

□

Теперь рассмотрим эти последовательности над кольцом классов вычетов.

Лемма 5. *Пусть* $q = r^k$, *где* r – *простое число,* $k > 1$, $r^{p_i-1} \not\equiv 1 \pmod{p_i^2}$, $i = 1, 2, \dots, m$, *и последовательность* u^∞ *определена по формуле* (7) *для* $v = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. *Тогда имеют место следующие оценки её линейной сложности:*

A. $L(u^\infty) \ge p_1^{k_1} p_2^{k_2} \dots p_m (p_m^{k_m-1} - 1)$, *когда* $r = 2$ *и* $k_m > 1$;

B. $L(u^\infty) \ge p_1^{k_1} p_2^{k_2} \dots p_{m-1}^{k_{m-1}}(p_m-1)(r-1)/r$, *если* $r = 2$ *и* $k_m = 1$ *или* $r > 2$.

Доказательство. По условию последовательность определена над конечным кольцом $\mathbb{Z}_{r^k}$. Значит, имеется естественный эпиморфизм $\psi(n) = n \bmod r$ из $\mathbb{Z}_{r^k}$ в $\mathbb{F}_r$. Применив этот эпиморфиз, получим последовательность $\psi(u^\infty) = (\psi(u_1), \psi(u_2), \psi(u_3), \dots)$ над $\mathbb{F}_r$. Для этой последовательности $\psi(u_i) = j$, если

$$i \bmod v \in \{\mathcal{F}_j, \mathcal{F}_{j+r}, \mathcal{F}_{j+2r}, \dots, \mathcal{F}_{j+(r^{k-1}-1)r}\}.$$

Значит, $\psi(u^\infty)$ – последовательность, определяемая по формуле (7) при замене e на er^{k-1} и замене q на r. Тогда теорема 1 и лемма 4 справедливы для $\psi(u^\infty)$. Отсюда получим оценку линейной сложности u^∞, так как $L(\psi(u^\infty)) \le L(u^\infty)$, и завершим доказательство леммы. □

Если q не является степенью простого числа, то можно получить оценку линейной сложности для каждого простого числа, входящего в разложение q, и воспользоваться китайской теоремой об остатках для оценки линейной сложности последовательности над $\mathbb{Z}_q$ в этом случае.

Заключение

Получены оценки линейной сложности как бинарных обобщенных циклотомических последовательностей, так и небинарных. Рассмотренные последовательности сформированы с применением обобщенных циклотомических классов по произвольному нечетному модулю $v = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$. Обобщены предыдущие результаты, полученные для $m = 1, 2$.

Благодарности. Исследование выполнено при финансовой поддержке Российского научного фонда, проект № 24–21–00442.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Список литературы

1. *Cusick T.W., Ding C., Renvall A.* Stream Ciphers and Number Theory. Ser.: North-Holland Mathematical Library. V. 55, Suppl. C. Amsterdam: Elsevier Sci., 1998. 431 p. URL: https://www.sciencedirect.com/bookseries/north-holland-mathematical-library/vol/55/suppl/C.

2. *Chen X., Chen Z., Liu H.* A family of pseudorandom binary sequences derived from generalized cyclotomic classes modulo $p^{m+1}q^{n+1}$ // Int. J. Network Secur. 2020. V. 22, No 4. P. 610–620. https://doi.org/10.6633/IJNS.202007_22(4).09.

3. *Fan C., Ge G.* A unified approach to Whiteman's and Ding–Helleseth's generalized cyclotomy over residue class rings // IEEE Trans. Inf. Theory. 2014. V. 60, No 2. P. 1326–1336. https://doi.org/10.1109/TIT.2013.2290694.

4. *Hu L., Yue Q., Wang M.* The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$ // IEEE Trans. Inf. Theory. 2012. V. 58, No 8. P. 5534–5543. https://doi.org/10.1109/TIT.2012.2196254.

5. *Zeng X., Cai H., Tang X., Yang Y.* Optimal frequency hopping sequences of odd length // IEEE Trans. Inf. Theory. 2013. V. 59, No 5. P. 3237–3248. https://doi.org/10.1109/TIT.2013.2237754.

6. *Xiao Z., Zeng X., Li C., Helleseth T.* New generalized cyclotomic binary sequences of period p^2 // Des. Codes Cryptogr. 2018. V. 86, No 7. P. 1483–1497. https://doi.org/10.1007/s12095-022-00569-4.

7. *Edemskiy V., Li C., Zeng X., Helleseth T.* The linear complexity of generalized cyclotomic binary sequences of period p^n // Des. Codes Cryptogr. 2019. V. 87, No 5. P. 1183–1197. https://doi.org/10.1007/s10623-018-0513-2.

8. *Ye Z., Ke P., Wu C.* A further study of the linear complexity of new binary cyclotomic sequence of length p^r // Appl. Algebra Eng. Commun. Comput. 2019. V. 30, No 3. P. 217–231. https://doi.org/10.1007/s00200-018-0368-9.

9. *Ouyang Y., Xie X.* Linear complexity of generalized cyclotomic sequences of period $2p^m$ // Des. Codes Cryptogr. 2019. V. 87, No 11. P. 2585–2596. https://doi.org/10.1007/s10623-019-00638-5.

10. *Edemskiy V., Wu C.* Linear complexity of generalized cyclotomic sequences with period $p^n q^m$ // Arithmetic of Finite Fields: 9th International Workshop, WAIFI 2022, Chengdu, China, August 29 – September 2, 2022, Revised Selected Papers / Mesnager S., Zhou Z. (Eds.). Ser.: Lecture Notes in Computer Science. V. 13638. Cham: Springer, 2023. P. 320–333. https://doi.org/10.1007/978-3-031-22944-2_21.

11. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.

Поступила в редакцию 5.05.2024
Принята к публикации 11.05.2024

Едемский Владимир Анатольевич, доктор физико-математических наук, доцент, заведующий кафедрой «Прикладной математики и информатики»

Новгородский государственный университет им. Ярослава Мудрого
ул. Большая Санкт-Петербургская, д. 41, г. Великий Новгород, 173003, Россия
E-mail: *vladimir.edemsky@novsu.ru*

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)

**UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)**

2024, vol. 166, no. 2, pp. 162–172

ORIGINAL ARTICLE
doi: 10.26907/2541-7746.2024.2.162-172

On the Linear Complexity of Generalized Cyclotomic Sequences with Odd Period

V.A. Edemskiy

Yaroslav-the-Wise Novgorod State University, Veliky Novgorod, 173003 Russia
E-mail: *vladimir.edemsky@novsu.ru*

Received May 5, 2024; Accepted May 11, 2024

Abstract

The linear complexity of new generalized cyclotomic sequences with odd period was estimated. The sequences were defined using generalized cyclotomic classes composite modulo. Conditions sufficient for the existence of binary and non-binary sequences with high linear complexity were obtained. The earlier results on the linear complexity of sequences with the period equal to the power of a prime were generalized.

Keywords: generalized cyclotomic sequences, linear complexity

Acknowledgements. This study was supported by the Russian Science Foundation (project no. 24-21-00442).

Conflicts of Interest. The author declares no conflicts of interest.

References

1. Cusick T.W., Ding C., Renvall A. *Stream Ciphers and Number Theory.* Ser.: North-Holland Mathematical Library. Vol. 55, Suppl. C. Amsterdam, Elsevier Sci., 1998. 431 p. URL: https://www.sciencedirect.com/bookseries/north-holland-mathematical-library/vol/55/suppl/C.

2. Chen X., Chen Z., Liu H. A family of pseudorandom binary sequences derived from generalized cyclotomic classes modulo $p^{m+1}q^{n+1}$. *Int. J. Network Secur.*, 2020, vol. 22, no. 4, pp. 610–620. https://doi.org/10.6633/IJNS.202007_22(4).09.

3. Fan C., Ge G. A unified approach to Whiteman's and Ding–Helleseth's generalized cyclotomy over residue class rings. *IEEE Trans. Inf. Theory*, 2014, vol. 60, no. 2, pp. 1326–1336. https://doi.org/10.1109/TIT.2013.2290694.

4. Hu L., Yue Q., Wang M. The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$. *IEEE Trans. Inf. Theory*, 2012, vol. 58, no. 8, pp. 5534–5543. https://doi.org/10.1109/TIT.2012.2196254.

5. Zeng X., Cai H., Tang X., Yang Y. Optimal frequency hopping sequences of odd length. *IEEE Trans. Inf. Theory*, 2013, vol. 59, no. 5, pp. 3237–3248. https://doi.org/10.1109/TIT.2013.2237754.

6. Xiao Z., Zeng X., Li C., Helleseth T. New generalized cyclotomic binary sequences of period p^2. *Des. Codes Cryptogr.*, 2018, vol. 86, no. 7, pp. 1483–1497. https://doi.org/10.1007/s10623-017-0408-7.

7. Edemskiy V., Li C., Zeng X., Helleseth T. The linear complexity of generalized cyclotomic binary sequences of period p^n. *Des. Codes Cryptogr.*, 2019, vol. 87, no. 5, pp. 1183–1197. https://doi.org/10.1007/s10623-018-0513-2.

8. Ye Z., Ke P., Wu C. A further study of the linear complexity of new binary cyclotomic sequence of length p^r. *Appl. Algebra Eng. Commun. Comput.*, 2019, vol. 30, no. 3, pp. 217–231. https://doi.org/10.1007/s00200-018-0368-9.

9. Ouyang Y., Xie X. Linear complexity of generalized cyclotomic sequences of period $2p^m$. *Des. Codes Cryptogr.*, 2019, vol. 87, no. 11, pp. 2585–2596. https://doi.org/10.1007/s10623-019-00638-5.

10. Edemskiy V., Wu C. Linear complexity of generalized cyclotomic sequences with period $p^n q^m$. In: Mesnager S., Zhou Z. (Eds.) *Arithmetic of Finite Fields: 9th International Workshop, WAIFI 2022, Chengdu, China, August 29 – September 2, 2022, Revised Selected Papers*. Ser.: Lecture Notes in Computer Science. Vol. 13638. Cham, Springer, 2023, pp. 320–333. https://doi.org/10.1007/978-3-031-22944-2_21.

11. Ireland K., Rosen M. *Klassicheskoe vvedenie v sovremennuyu teoriyu chisel* [A Classical Introduction to Modern Number Theory]. Moscow, Mir, 1987. 416 p. (In Russian)

⟨ ***Для цитирования:*** *Едемский В.А.* О линейной сложности обобщенных циклотомических последовательностей нечетного периода // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2024. Т. 166, кн. 2. С. 162–172.
URL: https//doi.org/10.26907/2541-7746.2024.2.162-172. ⟩

⟨ ***For citation:*** Edemskiy V.A. On the linear complexity of generalized cyclotomic sequences with odd period. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2024, vol. 166, no. 2, pp. 162–172.
URL: https//doi.org/10.26907/2541-7746.2024.2.162-172. (In Russian) ⟩