DOI: 10.24143/2072-9502-2021-1-70-79
УДК 519.7

АНАЛИЗ ЛИНЕЙНОЙ СЛОЖНОСТИ *Q*-ИЧНЫХ ОБОБЩЕННЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПЕРИОДА p^n [1]

В. А. Едемский

Новгородский государственный университет имени Ярослава Мудрого,
Великий Новгород, Российская Федерация

К рассмотрению предложен анализ линейной сложности периодических q-ичных последовательностей при изменении k их членов на периоде. Последовательности формируются с применением новой обобщенной циклотомии по модулю, равному степени нечетного простого числа. Получено рекуррентное соотношение и оценено изменение линейной сложности рассматриваемых последовательностей, когда q – примитивный корень по модулю, равному периоду последовательности. Из анализа результатов следует, что линейная сложность этих последовательностей существенно не уменьшается при k меньшем, чем половина периода. Исследование обобщает результаты для бинарного случая, полученные ранее.

Ключевые слова: *k*-ошибка линейной сложности, циклотомия, *q*-ичные последовательности.

Для цитирования: *Едемский В. А.* Анализ линейной сложности *q*-ичных обобщенных циклотомических последовательностей периода p^n // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2021. № 1. С. 70–79. DOI: 10.24143/2072-9502-2021-1-70-79.

Введение

Элементарная теория чисел, в частности циклотомия, применяется в теории кодирования и криптографии, при построении разностных множеств и формировании последовательностей.

Циклотомические классы определяются как классы смежности подгруппы мультипликативной группы обратимых элементов Z_N^* кольца классов вычетов Z_N по модулю N. Для составного N они называются обобщенными циклотомическими классами. Циклотомические и обобщенные циклотомические классы применяются при определении последовательностей. С криптографической точки зрения циклотомические и обобщенные циклотомические последовательности изучались в [1–3]. Свойства обобщенных циклотомических последовательностей длины p^n исследовались в [4–9]. Новый подход к определению обобщенных циклотомических классов предложен в [10], а в [11] на основе новой циклотомии из [10] сформированы бинарные последовательности с периодом p^n. Свойства этих последовательностей, в частности линейная сложность, изучены в [3, 11, 12]. Для криптографических применений последовательность должна иметь высокую линейную сложность, но это только необходимое условие. Важно, как она меняется при изменении нескольких членов последовательности. Наименьшая линейная сложность, которую можно получить, изменяя на периоде не более чем k членов исходной последовательности, называется k-ошибкой линейной сложности последовательности [13]. В [14] изучена k-ошибка линейной сложности отдельных новых обобщенных циклотомических бинарных последовательностей.

Определение бинарных последовательностей из [11] было расширено в [15], где предложено правило построения q-ичных последовательностей периода p^n на основе новой циклотомии. Рассмотренные в [15] последовательности имеют высокую линейную сложность над конечным полем порядка q.

Данная статья посвящена изучению k-ошибки линейной сложности последовательностей с периодом p^n из [15] и обобщению результатов из [14]. С этой целью для k-ошибки линейной сложности будет получена рекуррентная формула и ее оценка для ряда значений k.

Основные определения

[1] Исследование выполнено при финансовой поддержке РФФИ и ГФЕН Китая в рамках научного проекта № 19-51-53003.

В этом разделе напомним определение q-ичных последовательностей из [15].

Пусть p – простое число, отличное от двух, $p = ef + 1$, где e, f – целые положительные числа, и g – примитивный корень по модулю p^n [16].

Согласно [10], обобщенные циклотомические классы порядка d_j по модулю p^j определяются следующим образом:

$$D_i^{(p^j)} = \left\{ g^{i+t\cdot d_j} \pmod{p^j} \,|\, 0 \le t < e \right\}, \quad 0 \le i < d_j. \tag{1}$$

Здесь $j = 1, 2, ..., n$ и $d_j = \varphi(p^j)/e = p^{j-1}f$. Множества $D_i^{(p^j)}$, $i = 0, 1, ..., d_j - 1$ являются классами смежности $D_0^{(p^j)}$ и образуют разбиение $Z_{p^j}^*$ для каждого целого $j \ge 1$.

На основе этих классов в [11] сформировано новое семейство почти сбалансированных бинарных последовательностей, их линейная сложность изучена в [3, 11, 12], когда f – четное. В [15] предложено обобщение этой конструкции и рассмотрены новые q-ичные последовательности.

Пусть $H_0^{(p^j)} = \bigcup_{i=0}^{r_j-1} D_{(i+b)(\mathrm{mod}\, d_j)}^{(p^j)}$, $H_1^{(p^j)} = \bigcup_{i=r_j}^{2r_j-1} D_{(i+b)(\mathrm{mod}\, d_j)}^{(p^j)}$, ..., $H_{q-1}^{(p^j)} = \bigcup_{i=(q-1)r_j}^{qr_j-1} D_{(i+b)(\mathrm{mod}\, d_j)}^{(p^j)}$, а также

$$C_k^{(p^m)} = \bigcup_{j=1}^{m} p^{m-j} H_k^{(p^j)}, \; k = 0, 1, ..., q-1, \qquad m = 1, 2, ..., n,$$

где $q \,|\, f$, $b : 0 \le b < p^{n-1}f$ и $r_j = p^{j-1}f/q$.

Согласно определению $C_k^{(p^m)}$ имеем, что

$$Z_{p^m} = C_0^{(p^m)} \cup C_1^{(p^m)} \cup ... \cup C_{q-1}^{(p^m)} \cup \{0\} \text{ и } |\, C_j^{(p^m)} \,| = (p^m - 1)/q.$$

В [15] рассмотрено семейство q-ичных последовательностей $s^{(m)} = (s_0^{(m)}, s_1^{(m)}, s_2^{(m)}, ...)$ периода p^m, определенное по следующей формуле:

$$s_i^{(m)} = \begin{cases} 0, \text{ если } i \,(\mathrm{mod}\, p^m) \in C_0^{(p^m)} \cup \{0\}; \\ 1, \text{ если } i \,(\mathrm{mod}\, p^m) \in C_k^{(p^m)}. \end{cases} \tag{2}$$

Линейная сложность последовательности s над конечным полем $\mathbb{F}_q$ определяется как наименьшее натуральное число L, для которого существуют константы $c_1, ..., c_L$ из $\mathbb{F}_q$ такие, что выполняется рекуррентное соотношение $s_k = c_1 s_{k-1} + c_2 s_{k-2} + ... + c_L s_{k-L}$ для всех $k \ge L$.

В [15] показано, что новое семейство последовательностей обладет высокой линейной сложностью над конечным полем порядка q, $q > 2$, где q – простое число. В этой статье рассмотрим, как она меняется при изменении последовательности.

K-ошибка линейной сложности $LC_k^{\mathbb{F}_q}(s)$ последовательности $s = (s_0, s_1, ..., s_{N-1})$ периода N определеляется как $LC_k^{\mathbb{F}_q}(s) = \min_{\tau} LC(\tau)$, где минимум берется по всем *N*-периодическим последовательностям $\tau = (\tau_0, \tau_1, ..., \tau_{N-1})$ над $\mathbb{F}_q$, для которых расстояние Хэмминга между векторами $\mathbf{s} = (s_0, s_1, ..., s_{N-1})$ и $\boldsymbol{\tau} = (\tau_0, \tau_1, ..., \tau_{N-1})$ не превышает k.

Анализ k -ошибки линейной сложности последовательности

Основные результаты исследования представлены в следующей теореме.

Теорема. Пусть q – примитивный корень по модулю p^n и $s^{(n)}$ – последовательность периода p^n, определенная по (2). Тогда справедливы следующие утверждения для k-ошибки линейной сложности $LC_k^{\mathbb{F}_q}(s^{(n)})$ последовательности $s^{(n)}$:

$$1)\ LC_k^{\mathbb{F}_q}(s^{(n)}) = p^n - p^{n-1} + LC_k^{\mathbb{F}_q}(s^{(n-1)}), \text{ если } k < (p^{n-1}-1)(q-1)/q;$$

$$2)\ LC_k^{\mathbb{F}_q}(s^{(n)}) = p^n - p^{n-1}, \text{ если } (p^{n-1}-1)(q-1)/q \le k < p^{n-1}(p-1)(q-1)/q;$$

$$3)\ LC_k^{\mathbb{F}_q}(s^{(n)}) \le p^{n-1} \text{ при } k \ge p^{n-1}(p-1)(q-1)/q;$$

$$4)\ LC_k^{\mathbb{F}_q}(s^{(n)}) = 0 \text{ для } k \ge (p^n-1)(q-1)/q.$$

Таким образом, эти рассматриваемые последовательности имеют высокую линейную сложность, и она существенно не уменьшается при изменении k членов последовательности для $k < (p^{n-1}-1)(q-1)/q$. Следовательно, они стабильны.

Прежде чем доказать основную теорему, получим несколько вспомогательных утверждений. Порождающий многочлен последовательности $s^{(m)}$ обозначим через $S^{(m)}(x) = s_0 + s_1 x + ... + s_{p^m-1} x^{p^m-1}$. Хорошо известно, что k-ошибку линейной сложности $s^{(n)}$ над $\mathbb{F}_q$ можно найти, применяя следующее соотношение:

$$LC_k^{\mathbb{F}_q}(s^{(n)}) = \min_{0 \le wt(T(x)) \le k} \{p^n - \deg(\text{НОД}(x^{p^n}-1, S^{(n)}(x) + T(x)))\},$$

где $T(x) \in \mathbb{F}_q[x]$ – многочлен последовательности, корректирующей $s^{(n)}$ (т. е. если $s_i^{(n)}$ меняется, то $t_i \ne 0$, иначе $t_i = 0$). Здесь вес многочлена, т. е. число его ненулевых коэффициентов, обозначается через $wt(-)$.

В разделе «Анализ k-ошибки линейной сложности последовательности» сначала получим рекуррентную формулу для порождающих многочленов рассматриваемых последовательностей и докажем некоторые вспомогательные утверждения о многочлене корректирующей последовательности.

1. Рекуррентная формула. Обозначим $d_i^{(j)}(x) = \sum_{t \in D_{(i+b) (\mathrm{mod} d_j)}^{(p^j)}} x^t$, $j = 1, 2, ..., n$, $i = 0, 1, ..., d_j - 1$ и $h_l^{(j)}(x) = \sum_{i=lr_j}^{(l+1)r_j - 1} d_i^{(j)}(x)$, $l = 0, 1, ..., q-1$. Заметим, что индексы i в $d_i^{(j)}(x)$ всегда вычисляются по модулю d_j. В оставшейся части статьи значения индексов по модулю будут опускаться, если это не вызовет затруднений. Из формул (1), (2) получаем, что

$$S^{(m)}(x) = \sum_{i=0}^{p^m-1} s_i x^i = \sum_{l=0}^{q-1} l \sum_{t \in C_l^{(p^m)}} x^t = \sum_{l=0}^{q-1} l \sum_{j=1}^{m} h_l^{(j)}(x^{p^{m-j}}). \qquad (3)$$

Предварительно докажем две леммы, необходимые для получения рекуррентной формулы. Свойства $D_i^{(p^j)}$ изучены в [11, 12]. Согласно [12] имеем следующее утверждение.

Лемма 1. Пусть $D_i^{(p^j)}$ определены по формуле (1), и $j = 2, ..., n$. Тогда

$$1)\ D_i^{(p^j)} (\mathrm{mod}\, p^{j-1}) = D_{i (\mathrm{mod} d_{j-1})}^{(p^{j-1})};$$

$$2)\ p^{n-j} D_i^{(p^j)} (\mathrm{mod}\, p^{n-1}) = p^{n-j} D_{i (\mathrm{mod} d_{j-1})}^{(p^{j-1})}.$$

Лемма 2. Пусть $d_i^{(j)}(x)=\sum_{t\in D^{(p^j)}_{(i+b)(\mathrm{mod}\, d_j)}} x^t$, $h_l^{(j)}(x)=\sum_{i=lr_j}^{(l+1)r_j-1} d_i^{(j)}(x)$ и $j=2,...,n$, тогда

$$1)\ d_i^{(1)}(x^{p^{n-1}})(\mathrm{mod}\, x^{p^{n-1}}-1)=e;$$

$$2)\ d_i^{(j)}(x^{p^{n-j}})(\mathrm{mod}\, x^{p^{n-1}}-1)=d^{(j-1)}_{i(\mathrm{mod}\, d_{j-1})}(x^{p^{n-j}});$$

$$3)\ h_l^{(1)}(x^{p^{n-1}})(\mathrm{mod}\, x^{p^{n-1}}-1)=er_1;$$

$$4)\ h_l^{(j)}(x^{p^{n-j}})(\mathrm{mod}\, x^{p^{n-1}}-1)=h_l^{(j-1)}(x^{p^{n-j}})+(p-1)/q\cdot\sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(x^{p^{n-j}}).$$

Доказательство:

1) очевидно, т. к. $|D_i^{(p)}|=e$;

2) по определению $d_i^{(j)}(x^{p^{n-j}})=\sum_{l\in D_i^{(p^j)}} x^{lp^{n-j}}=\sum_{l\in p^{n-j}D_i^{(p^j)}} x^l$. Так как, по лемме 1, $p^{n-j}D_i^{(p^j)}(\mathrm{mod}\, p^{n-1})=p^{n-j}D^{(p^{j-1})}_{i(\mathrm{mod}\, d_{j-1})}$, то $d_i^{(j)}(x^{p^{n-j}})(\mathrm{mod}\, x^{p^{n-1}}-1)=\sum_{l\in p^{n-j}D^{(p^{j-1})}_{i(\mathrm{mod}\, d_{j-1})}} x^l=\sum_{l\in D^{(p^{j-1})}_{i(\mathrm{mod}\, d_{j-1})}} x^{lp^{n-j}}=$

$=d^{(j-1)}_{i(\mathrm{mod}\, d_{j-1})}(x^{p^{n-j}})$;

3) воспользовавшись формулой $d_i^{(1)}(x^{p^{n-1}})(\mathrm{mod}\, x^{p^{n-1}}-1)=e$, получаем, что $h_l^{(1)}(x^{p^{n-1}})(\mathrm{mod}\, x^{p^{n-1}}-1)=er_1$;

4) по 1) и формуле для $h_l^{(j)}(x)$ видим, что

$$h_l^{(j)}(x^{p^{n-j}})(\mathrm{mod}\, x^{p^{n-1}}-1)=\sum_{i=lr_j}^{(l+1)r_j-1} d^{(j-1)}_{i(\mathrm{mod}\, d_{j-1})}(x^{p^{n-j}}).$$

Здесь $r_j=(p-1)r_{j-1}+r_{j-1}$ и $d_{j-1}=p^{j-2}f=r_{j-1}q$, значит $r_j=(p-1)d_{j-1}/q+r_{j-1}$. В итоге

$$\sum_{i=lr_j}^{(l+1)r_j-1} d^{(j-1)}_{i(\mathrm{mod}\, d_{j-1})}(x^{p^{n-j}})=\sum_{i=lr_j}^{(l+1)r_{j-1}-1} d^{(j-1)}_{i(\mathrm{mod}\, d_{j-1})}(x^{p^{n-j}})+(p-1)/q\cdot\sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(x^{p^{n-j}})$$

или

$$h_l^{(j)}(x^{p^{n-j}})(\mathrm{mod}\, x^{p^{n-1}}-1)=h_l^{(j-1)}(x^{p^{n-j}})+(p-1)/q\cdot\sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(x^{p^{n-j}}).$$

Доказательство леммы 2 завершено.

Утверждение 1. Пусть $s^{(n)}$ – последовательность, определенная по формуле (2). В этом случае для $n\ge 2$ выполняется рекуррентное соотношение

$$S^{(n)}(x)(\mathrm{mod}\, x^{p^{n-1}}-1)=S^{(n-1)}(x).$$

Доказательство. Согласно (3) имеем, что

$$S^{(n)}(x)\equiv\sum_{l=0}^{q-1} l\sum_{j=1}^{n} h_l^{(j)}(x^{p^{n-j}})(\mathrm{mod}\, X^{p^{n-1}}-1).$$

В силу леммы 2 получаем, что

$$S^{(n)}(X)(\mathrm{mod}\, X^{p^{n-1}}-1)=\sum_{l=0}^{q-1} l\sum_{j=2}^{n}\left(h_l^{(j-1)}(x^{p^{n-j}})+(p-1)/q\cdot\sum_{i=0}^{d_{j-1}-1} d_i^{(j-1)}(x^{p^{n-j}})\right)+$$
$$+\ er_1(1+2+...+q-1).$$

Из равенства

$$\sum_{l=0}^{q-1} l \sum_{j=2}^{n} \sum_{i=0}^{d_{j-1}} d_i^{(j-1)} (x^{p^{n-j}}) = \sum_{j=2}^{n} \sum_{i=0}^{d_{j-1}} d_i^{(j-1)} (x^{p^{n-j}}) \sum_{l=0}^{q-1} l = 0$$

в $\mathbb{F}_q$, опять по лемме 2, видим, что

$$S^{(n)}(X) (\mathrm{mod}\, X^{p^{n-1}} - 1) = \sum_{l=0}^{q-1} l \sum_{j=2}^{n} h_l^{(j-1)} (x^{p^{n-j}}) = S^{(n-1)}(x),$$

что и требовалось доказать.

Заметим, что при $q = 2$ это утверждение истинно только для $p \equiv 1 (\mathrm{mod}\, 4)$ [14].

2. Оценка k-ошибки линейной сложности последовательности. Пусть $\Phi_m(x) = x^{(p-1)p^{m-1}} + ... + x^{p^{m-1}} + 1$. В этом подразделе изучим, когда $S^{(m)}(X)$ делится на $\Phi_m(x)$.

Предварительно обсудим некоторые леммы.

Лемма 3. Пусть $v \in D_j^{(p^{m-1})}$ для $m > 1$ и $U_v = \{v, v + p^{m-1}, ..., v + (p-1)p^{m-1}\}$. Тогда

$$|U_v \cap D_i^{(p^m)}| = \begin{cases} 1, & \text{если } i \equiv j (\mathrm{mod}\, fp^{m-2}); \\ 0 & \text{иначе.} \end{cases}$$

Доказательство. По условию $v \in D_j^{(p^{m-1})}$, т. е. $v = g^{j + hd_{m-1}} (\mathrm{mod}\, p^{m-1})$ для целого $h : 0 \le h < e$.

Предположим, что $v + ap^{m-1} \in D_i^{(p^m)}$ для $a : 0 \le a \le p-1$. В этом случае $v + ap^{m-1} \equiv g^{i+ud_m} (\mathrm{mod}\, p^m)$ для целого $u : 0 \le u < e$. Тогда $g^{j+hd_{m-t1}} \equiv g^{i+ud_m} (\mathrm{mod}\, p^{m-1})$ и $j + hd_{m-1} \equiv i + ud_m (\mathrm{mod}\, (p-1)p^{m-2})$. Так как $p - 1 = ef$ и $d_{m-1} = p^{m-2} f$, то $i - j \equiv 0 (\mathrm{mod}\, fp^{m-2})$. Таким образом, $|U_v \cap D_i^{(p^m)}| = 0$ для $i \not\equiv j (\mathrm{mod}\, fp^{m-2})$.

Далее, пусть $v + ap^{m-1} \in D_i^{(p^m)}$ и $v + bp^{m-1} \in D_i^{(p^m)}$, где $a \ne b$, $a, b = 0, 1, ..., p-1$, тогда $v + ap^{m-1} \equiv g^{i+ud_m} (\mathrm{mod}\, p^m)$ и $v + bp^{m-1} \equiv g^{i+zd_m} (\mathrm{mod}\, p^m)$ для $u, z : 0 \le u, z < e$. Следовательно, $g^{i+ud_m} \equiv g^{i+zd_m} (\mathrm{mod}\, p)$ и $(u - z)d_m$ делится на $p - 1$. Последнее утверждение невозможно для $u \ne z : 0 \le u, z < e$.

Таким образом, $|U_v \cap D_i^{(p^m)}| \le 1$ для $i \equiv j (\mathrm{mod}\, fp^{m-2})$. Так как $|U_v| = p$ и $|\{i \,|\, i \equiv j (\mathrm{mod}\, fp^{m-2}), i = 0, 1, ..., p^{m-1} f - 1\}| = p$, то $|U_v \cap D_i^{(p^m)}| = 1$ для $i \equiv j (\mathrm{mod}\, fp^{m-2})$.

Следствие. Если $m > 1$, то

$$|U_v \cap H_l^{(p^m)}| = \begin{cases} (p-1)/q + 1, & \text{если } v \in H_l^{(p^{m-1})}; \\ (p-1)/q & \text{иначе.} \end{cases}$$

Лемма 4. Если $a = 1, 2, ..., q-1$, то

$$wt\left(a(x^v + x^{v+p^{m-1}} + ... + x^{v+(p-1)p^{m-1}}) - \sum_{l=0}^{q-1} l h_l^{(m)}(x) \right) =$$

$$= \begin{cases} er_m(q-1) + 1, & \text{если } v \in H_0^{(p^{m-1})}; \\ er_m(q-1), & \text{если } v \in H_j^{(p^{m-1})} \text{ и } a \ne j; \\ er_m(q-1) - 1, & \text{если } v \in H_j^{(p^{m-1})} \text{ и } a = j. \end{cases}$$

Доказательство. Очевидно, что

$$wt\left(a(x^v + x^{v+p^{m-1}} + ... + x^{v+(p-1)p^{m-1}}) - \sum_{l=0}^{q-1} lh_l^{(m)}(x) \right) = \sum_{l=0}^{q-1} wt\left(a \sum_{i \in U_v \cap H_l^{(p^{m-1})}} x^i - lh_l^{(m)}(x) \right),$$

где $U_v = \{v, v+p^{m-1}, ..., v+(p-1)p^{m-1}\}$, как и ранее.

Пусть $v \in U_v \cap H_0^{(p^{m-1})}$, тогда, по следствию, $wt\left(a\sum_{i \in U_v \cap H_l^{(p^{m-1})}} x^i\right) = (p-1)/q + 1$, и для $l > 0$ имеем, что

$$wt\left(a \sum_{i \in U_v \cap H_l^{(p^{m-1})}} x^i - lh_l^{(m)}(x) \right) = \begin{cases} er_m, & \text{если } l \neq a; \\ er_m - (p-1)/q, & \text{если } l = a. \end{cases}$$

Суммируя, получаем утверждение леммы для $v \in U_v \cap H_0^{(p^{m-1})}$.

Предположим, что $v \in U_v \cap H_j^{(p^{m-1})}, j > 0$. Тогда, опять по следствию 1 видим, что

$$wt\left(a \sum_{i \in U_v \cap H_l^{(p^{m-1})}} x^i - lh_l^{(m)}(x) \right) = \begin{cases} (p-1)/q, & \text{если } l = 0; \\ er_m, & \text{если } l \neq a; \\ er_m - (p-1)/q - 1, & \text{если } l = j, l = a. \end{cases}$$

Снова суммируя, получаем утверждение этой леммы для $v \in U_v \cap H_j^{(p^{m-1})}, j > 0$.

Лемма 5. Пусть $f_m(x)$ – многочлен, такой что $\sum_{l=0}^{q-1} lh_l^{(m)}(x) + f_m(x)$ делится на $\Phi_m(x)$ для $m > 1$. Тогда

$$\min wt(f_m(X)) = p^{m-2}(p-1)^2(q-1)/q.$$

Доказательство. По условию

$$\sum_{l=0}^{q-1} lh^{(m)}(x) + f_m(x) = \left(x^{(p-1)p^{m-1}} + ... + x^{p^{m-1}} + 1 \right) f(x),$$

где $a_i \in \mathbb{F}_q$ и $f(x) = a_1 x^{t_1} + a_2 x^{t_2} + ... + a_h x^{t_h}, 0 < t_j < p^{m-1}, j = 1, 2, ..., h$, $h < p^{m-1}$. Не нарушая общности, можем предположить, что $t_i \not\equiv 0 (\mathrm{mod}\, p)$. Тогда

$$f_m(x) = \sum_{i=1}^{h} a_i \left(x^{t_i} + x^{t_i + p^{m-1}} + ... + x^{t_i + (p-1)p^{m-1}} \right) - \sum_{l=0}^{q-1} lh_l^{(m)}(x).$$

Пусть $k_l = |\{a_i \mid a_i = l, t_i \in H_l^{(p^{m-1})} i = 1, 2, ..., h\}$. Согласно лемме 4 получаем, что

$$wt(f_m(x)) \geq (q-1)er_m - \sum_{l=1}^{q-1} k_l$$

и

$$\sum_{l=1}^{q-1} k_l = \sum_{l=1}^{q-1} |H_l^{(p^{m-1})}|.$$

Так как $r = p^{m-1} f / q$, то

$$wt(f_m(x)) \ge p^{m-1}(p-1)(q-1)/q - p^{m-2}(p-1)(q-1)/q = p^{m-2}(p-1)^2(q-1)/q.$$

Теперь покажем, что существует многочлен $f_m(X)$, удовлетворяющий условиям леммы, вес которого равен полученной выше оценке. Возьмем

$$f_m(x) = \sum_{l=1}^{q-1} l \left(\sum_{i \in H_l^{(p^{m-1})}} (x^i + x^{p^{m-1}} + ... + x^{(p-1)p^{m-1}}) - h_l^{(m)}(x) \right).$$

Тогда, по лемме 4, $wt(f_m(x)) = (q-1)er_m - p^{m-2}(p-1)(q-1)/q = p^{m-2}(p-1)^2(q-1)/q$. Очевидно, что

$$\sum_{l=0}^{q-1} h^{(m)}(x) + f_m(X) \equiv 0 (\mathrm{mod}\, X^{(p-1)p^{m-1}} + ... + X^{p^{m-1}} + 1).$$

Лемма 5 доказана.

Замечание. Для $q = 2$ это утверждение доказано в [14] другим способом.

Утверждение 2. Пусть $S^{(m)}(x) + E^{(m)}(x) \equiv 0 (\mathrm{mod}\, \Phi_m(x))$. Тогда наименьший возможный вес многочлена $E^{(m)}(x))$ равен $p^{m-1}(p-1)(q-1)/q$.

Доказательство. Из (3) получаем, что

$$S^{(m)}(x) = \sum_{l=0}^{q-1} l \sum_{j=1}^{m} h_l^{(j)}(x^{p^{m-j}}) = \sum_{l=0}^{q-1} l h_l^{(m)}(x) + S^{(m-1)}(x^p). \quad (4)$$

Будем доказывать это утверждение методом математической индукции.

1. Пусть $m = 1$. В этом случае $S^{(1)}(x) + E^{(1)}(x) \equiv 0 (\mathrm{mod}\, X^{p-1} + ... + X + 1)$. Ясно, что тогда $\min wt(E^{(1)}(X)) = (p-1)(q-1)/q$.

2. Предположим, что утверждение истинно для $S^{(m)}(x)$, т. е. существует многочлен $E^{(m)}(x)$ с весом $wt(E^{(m)}(x)) = p^{m-1}(p-1)(q-1)/q$ такой, что $S^{(m)}(x) + E^{(m)}(x)$ делится на $x^{(p-1)p^{m-1}} + ... + x^{p^{m-1}} + 1$. Тогда $S^{(m)}(x^p) + E^{(m)}(x^p)$ делится на $x^{(p-1)p^m} + ... + x^{p^m} + 1$ и $\min wt(E^{(m)}(x^p)) = p^{m-1}(p-1)(q-1)/q$.

Далее, предположим, что $S^{(m+1)}(x) + E^{(m+1)}(x)$ делится на $x^{(p-1)p^m} + ... + x^{p^m} + 1$. Тогда существует многочлен $R(x)$ такой, что

$$S^{(m+1)}(x) + E^{(m+1)}(x) = \left(X^{(p-1)p^m} + ... + x^{p^m} + 1 \right) R(x)$$

и $\deg R(x) < p^m$.

Пусть $E^{(m+1)}(x) = \sum_{i=0}^{p^{m+1}-1} e_i x^i$ и $R(x) = \sum_{i=0}^{p^{m+1-t}-1} r_i x^i$. Определим множества $E_0 = \{e_i \mid e_i \ne 0$ и $e_i \equiv 0 (\mathrm{mod}\, p)\}$, $E_1 = \{e_i \mid e_i \ne 0$ и $e_i \not\equiv 0 (\mathrm{mod}\, p)\}$, $R_0 = \{r_i \mid r_i \ne 0$ и $r_i \equiv 0 (\mathrm{mod}\, p)\}$ и $R_1 = \{r_i \mid r_i \ne 0$ и $r_i \not\equiv 0 (\mathrm{mod}\, p)\}$. Введем вспомогательные полиномы $E_0(x^p) = \sum_{pi \in E_0} x^{pi}$, $E_1(x) = \sum_{i \in E_1} x^i$, $R_0(x^p) = \sum_{pi \in R_0} x^{pi}$ и $R_1(x) = \sum_{i \in R_1} x^i$.

Тогда, согласно (4),

$$\sum_{l=0}^{q-1} l h_l^{(m)}(x) + E_1(x) + S^{(m)}(x^p) + E_0(x^p) =$$

$$= \left(x^{(p-1)p^m} + ... + x^{p^m} + 1 \right) R_1(x) + \left(X^{(p-1)p^m} + ... + x^{p^m} + 1 \right) R_0(x).$$

Следовательно,

$$\sum_{l=0}^{q-1} lh_l^{(m)}(x) + E_1(x) = \left(x^{(p-1)p^m} + ... + X^{p^m} + 1\right) R_1(x)$$

и

$$S^{(m)}(x^p) + E_0(x^p) = \left(x^{(p-1)p^m} + ... + x^{p^m} + 1\right) R_0(x).$$

Таким образом, по лемме 5 и индукционному предположению, $\min wt(E_1(x)) = p^{m-1}(p-1)(q-1)/q$ и $\min wt(E_0(x^p)) = p^{m-2}(p-1)(q-1)/q$. Окончательно, $\min wt(E^{(m+1)}(x)) = p^m(p-1)(q-1)/q$. Существование $E^{(m+1)}(x)$ с таким весом ясно из леммы 5. Утверждение 2 доказано.

Доказательство основной теоремы

По определению $\Phi_0(x), \Phi_1(x), ..., \Phi_n(x)$, справедливо следующее разложение

$$x^{p^n} - 1 = \Phi_0(x)\Phi_1(x) ... \Phi_n(x),$$

где $\Phi_0(X) = x - 1$, $\Phi_j(x) = 1 + x^{p^{j-1}} + x^{2p^{j-1}} + ... + x^{(p-1)p^{j-1}}$, $j = 1, 2, ..., n$.

Многочлены $\Phi_0(x), \Phi_1(x), ..., \Phi_n(x)$ неприводимы над $\mathbb{F}_q$, когда q – первообразный корень по модулю p^n [17].

1) Рассмотрим случай, когда $k < p^{n-1}(p-1)(q-1)/q$. По утверждению 2 здесь $\Phi_n(X) \nmid (S^{(n)}(x) + E^{(n)}(x))$ для любого $E^{(n)}(x)$ с весом $wt(E^{(n)}(x)) = k < p^{n-1}(p-1)(q-1)/q$. Таким образом, в силу утверждения 1, исследование $LC_k^{\mathbb{F}_q}(s^{(n)})$ сводится к изучению $LC_k^{\mathbb{F}_q}(s^{(n-1)})$.

Если $S^{(n-1)}(x) + E^{(n)}(x))$ делится на $G(x)$, тогда, по утверждению 1, видим, что $G(x)$ делит $S^{(n)}(x) + E^{(n)}(x))$, и наоборот. Отсюда получаем, что $LC_k^{\mathbb{F}_q}(s^{(n)}) = p^n - p^{n-1} + LC_k^{\mathbb{F}_q}(s^{(n-1)})$ для $k < p^{n-1}(p-1)(q-1)/q$.

2) Если $k \geq (p^{n-1} - 1)(q-1)/q$, тогда $LC_k^{\mathbb{F}_q}(s^{(n-1)}) = 0$ и $LC_k^{\mathbb{F}_q}(s^{(n)}) = p^n - p^{n-1}$.

3) Пусть $k \geq p^{n-1}(p-1)(q-1)/q$. Тогда, по утверждению 2, имеем многочлен $E^{(n)}(X)$ с весом $wt(E^{(n)}(x)) = p^{n-1}(p-1)(q-1)/q$ такой, что $(S^{(n)}(x) + E^{(n)}(x))$ делится на $\Phi_n(X)$.

Утверждение 4) очевидно.

Заключение

Исследована *k*-ошибка линейной сложности *q*-ичных последовательностей, полученных из новых обобщенных циклотомических классов по модулю, равному степени нечетного простого числа, когда *q* – примитивный корень по этому модулю. Получены рекуррентное соотношение и оценка для *k*-ошибки линейной сложности последовательностей. Результаты показывают, что *k*-ошибка линейной сложности рассматриваемых последовательностей существенно не уменьшается при $k < (p^{n-1} - 1)(q-1)/q$. Исследование обобщает результаты для бинарного случая, полученные ранее.

СПИСОК ЛИТЕРАТУРЫ

1. *Cusick T., Ding C., Renvall A.* Stream Ciphers and Number Theory. Elsevier Science, 2004. 446 p.

2. *Ding C., Helleseth T.* New generalized cyclotomy and its applications // Finite Fields and Their Applications. 1998. V. 4 (2). P. 140–166.

3. *Ye Z., Ke P., Wu C.* A further study of the linear complexity of new binary cyclotomic sequence of length p^n // AAECC. 2019. V. 30. N. 3. P. 217–223.

4. *Гантмахер В. Е., Быстров Н. Е., Чеботарев Д. В.* Шумоподобные сигналы. Анализ, синтез, обработка. СПб.: Наука и техника, 2005. 400 с.

5. *Du X., Chen Z.* A generalization of the Hall's sextic residue sequences // Information Sciences. 2013. V. 222. P. 784–794.

6. *Edemskiy V*. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1} // Designs, Codes and Cryptography. 2011. V. 61. N. 3. P. 251–260.

7. *Kim Y. J., Song H. Y*. Linear complexity of prime n-square sequences // 2008 IEEE International Symposium on Information Theory (Toronto, Ontario, Canada, July 6-11, 2008). Google Scholar, 2008. P. 2405–2408.

8. *Wu C., Chen Z., Du X*. The linear complexity of q-ary generalized cyclotomic sequences of period p^m // Journal of Wuhan University. 2013. V. 59. N. 2. P. 129–136.

9. *Yan T., Li S., Xiao G*. On the linear complexity of generalized cyclotomic sequences with the period p^m // Applied Mathematics Letters. 2008. V. 21. N. 2. P. 187–193.

10. *Zeng X., Cai H., Tang X., Yang Y*. Optimal frequency hopping sequences of odd length // IEEE Transactions on Information Theory. 2013. V. 59. N. 5. P. 3237–3248.

11. *Xiao Z., Zeng X., Li C., Helleseth T*. New generalized cyclotomic binary sequences of period p^2 // Designs, Codes and Cryptography. 2018. V. 86. N. 7. P. 1483–1497.

12. *Edemskiy V., Li C., Zeng X., Helleseth T*. The linear complexity of generalized cyclotomic binary sequences of period p^n // Designs, Codes and Cryptography. 2019. V. 87. N. 5. P. 1183–1197.

13. *Stamp M., Martin C.* An algorithm for the *k*-error linear complexity of binary sequences with period 2*n* // IEEE Transactions on Information Theory. 1993. V. 39. N. 4. P. 1398–1401.

14. *Chen Z., Edemskiy V., Ke P., Wu C.* On k-error linear complexity of pseudorandom binary sequences derived from Euler quotients // Adv. In Math. of Comm. 2018. V. 12. N. 4. P. 805–816.

15. *Edemskiy V., Sokolovskiy N*. The linear complexity of new *q*-ary generalized cyclotomic sequences of period p^n // MATEC Web of Conferences. 2019. V. 292. 02001.

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

17. *Лидл Р., Нидеррайтер Г*. Конечные поля. М.: Мир, 1988. 820 с.

Статья поступила в редакцию 14.11.2020

ИНФОРМАЦИЯ ОБ АВТОРЕ

Едемский Владимир Анатольевич – Россия, 173003, Великий Новгород; Новгородский государственный университет имени Ярослава Мудрого; д-р физ.-мат. наук, доцент; профессор кафедры прикладной математики и информатики; Vladimir.edemsky@nivsu.ru.

ANALYSIS OF LINEAR COMPLEXITY OF GENERALIZED CYCLOTOMIC Q -ARY SEQUENCES OF p^n PERIOD

V. A. Edemskiy

Yaroslav-the-Wise Novgorod State University,
Veliky Novgorod, Russian Federation

Abstract. The article presents the analysis of the linear complexity of periodic *q*-ary sequences when changing *k* of their terms per period. Sequences are formed on the basis of new generalized cyclotomy modulo equal to the degree of an odd prime. There has been obtained a recurrence relation and an estimate of the change in the linear complexity of these sequences, where *q* is a primitive root modulo equal to the period of the sequence. It can be inferred from the results that the linear complexity of these sequences does not sign ificantly decrease when *k* is less than half the period. The study summarizes the results for the binary case obtained earlier.

Key words: *k*-error of linear complexity, cyclotomy, *q*-ary sequences.

For citation: Edemskiy V. A. Analysis of linear complexity of generalized cyclotomic Q-ary sequences of p^n period. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2021;1:70-79. (In Russ.) DOI: 10.24143/2072-9502-2021-1-70-79.

REFERENCES

1. Cusick T., Ding C., Renvall A. *Stream Ciphers and Number Theory*. Elsevier Science, 2004. 446 p.

2. Ding C., Helleseth T. New generalized cyclotomy and its applications. *Finite Fields and Their Applications*, 1998, vol. 4 (2), pp. 140-166.

3. Ye Z., Ke P., Wu C. A further study of the linear complexity of new binary cyclotomic sequence of length p^n. *AAECC*, 2019, vol. 30, no. 3, pp. 217-223.

4. Gantmakher V. E., Bystrov N. E., Chebotarev D. V. *Shumopodobnye signaly. Analiz, sintez, obrabotka* [Pseudonoise signals. Analysis, synthesis, processing]. Saint-Petersburg, Nauka i tekhnika Publ., 2005. 400 p.

5. Du X., Chen Z. A generalization of the Hall's sextic residue sequences. *Information Sciences*, 2013, vol. 222, pp. 784-794.

6. Edemskiy V. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}. *Designs, Codes and Cryptography*, 2011, vol. 61, no. 3, pp. 251-260.

7. Kim Y. J., Song H. Y. Linear complexity of prime n-square sequences. *2008 IEEE International Symposium on Information Theory (Toronto, Ontario, Canada, July 6-11, 2008).* Google Scholar, 2008. Pp. 2405-2408.

8. Wu C., Chen Z., Du X. The linear complexity of q-ary generalized cyclotomic sequences of period p^m. *Journal of Wuhan University*, 2013, vol. 59, no. 2, pp. 129-136.

9. Yan T., Li S., Xiao G. On the linear complexity of generalized cyclotomic sequences with the period p^m. *Applied Mathematics Letters*, 2008, vol. 21, no. 2, pp. 187-193.

10. Zeng X., Cai H., Tang X., Yang Y. Optimal frequency hopping sequences of odd length. *IEEE Transactions on Information Theory*, 2013, vol. 59, no. 5, pp. 3237-3248.

11. Xiao Z., Zeng X., Li C., Helleseth T. New generalized cyclotomic binary sequences of period p^2. *Designs, Codes and Cryptography*, 2018, vol. 86, no. 7, pp. 1483-1497.

12. Edemskiy V., Li C., Zeng X., Helleseth T. The linear complexity of generalized cyclotomic binary sequences of period p^n. *Designs, Codes and Cryptography*, 2019, vol. 87, no. 5, pp. 1183-1197.

13. Stamp M., Martin C. An algorithm for the *k*-error linear complexity of binary sequences with period 2*n*. *IEEE Transactions on Information Theory*, 1993, vol. 39, no. 4, pp. 1398-1401.

14. Chen Z., Edemskiy V., Ke P., Wu C. On k-error linear complexity of pseudorandom binary sequences derived from Euler quotients. *Advances in Mathematics of Communications*, 2018, vol. 12, no. 4, pp. 805-816.

15. Edemskiy V., Sokolovskiy N. The linear complexity of new q-ary generalized cyclotomic sequences of period p^n. *MATEC Web of Conferences*, 2019, vol. 292, 02001.

16. Aierlend K., Rouzen M. *Klassicheskoe vvedenie v sovremennuiu teoriiu chise*l [Classical principles of modern theory of numbers]. Moscow, Mir Publ., 1987. 416 p.

17. Lidl R., Niderraiter G. *Konechnye polia* [Finite fields]. Moscow, Mir Publ., 1988. 820 p.

The article submitted to the editors 14.11.2020

INFORMATION ABOUT THE AUTHOR

Edemskiy Vladimir Anatolevich – Russia, 173003, Veliky Novgorod; Yaroslav-the-Wise Novgorod State University; Doctor of Physics and Mathematics, Assistant Professor; Professor of the Department of Applied Mathematics and Information Science; Vladimir.edemsky@nivsu.ru.