ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 3**

УДК 621.391.15

© 2019 г. **Л. Ли, Ш. Чжу, Л. Лю, С. Кай**

НЕКОТОРЫЕ q-ИЧНЫЕ ЦИКЛИЧЕСКИЕ КОДЫ ПО ЯВНЫМ МОНОМАМ НАД $\mathbb{F}_{q^m}$ [1]

Циклические коды как подкласс линейных кодов имеют практически значимые применения в системах связи, бытовой электронике и системах хранения информации благодаря наличию эффективных алгоритмов их кодирования и декодирования. Целью настоящей статьи является построение некоторых циклических кодов с помощью подхода, основанного на последовательностях. Точнее говоря, найдены размерность и порождающие многочлены для трех классов q-ичных циклических кодов, задаваемых некоторыми последовательностями с явными многочленами над $\mathbb{F}_{q^m}$. Также обсуждается минимальное расстояние таких циклических кодов. Некоторые из этих классов оптимальны согласно таблицам кодов. Кроме того, третий класс циклических кодов дает некоторые ответы на открытую проблему 3, поставленную Дином и Чжоу в [1].

Ключевые слова: циклические коды, последовательности, размерность кода, порождающий многочлен.

DOI: 10.1134/S0555292319030057

§ 1. Введение

Пусть $\mathbb{F}_q$ – конечное поле с $q = p^m$ элементами, где p – простое, а $m \geqslant 1$. Линейный $[n, k, d]$-код над конечным полем $\mathbb{F}_q$ называется циклическим, если для любого кодового слова $(c_0, c_1, \ldots, c_{n-1}) \in C$ также $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. Хорошо известно, что каждый циклический код длины n над $\mathbb{F}_q$ можно рассматривать как идеал кольца главных идеалов $\mathbb{F}_q[x]/(x^n - 1)$. Пусть $C = (g(x))$ – циклический код над $\mathbb{F}_q$ длины n, где $g(x)$ – нормированный многочлен наименьшей степени в C. Тогда $g(x)$ называется порождающим многочленом кода C, а $h(x) = \dfrac{x^n - 1}{g(x)} \in \mathbb{F}_q[x]$ – проверочным многочленом кода C. Далее, двойственный к C код определяется как

$$C^\perp = \{x \in \mathbb{F}_q^n : \, x \cdot y = 0, \, \forall\, y \in C\},$$

где через $x \cdot y$ обозначено евклидово скалярное произведение векторов x и y. Тогда $C^\perp = (h(x)^*)$, где $h(x)^* = h(0)^{-1} x^{\deg(h(x))} h(x^{-1})$ – взаимный к $h(x)$ многочлен.

Линейный $[n, k, d]$-код над $\mathbb{F}_q$ называется оптимальным, если его параметры лежат на какой-либо границе для линейных кодов. Линейный $[n, k, d]$-код над $\mathbb{F}_q$ называется почти оптимальным, если оптимален некоторый линейный код с параметрами $[n, k, d + 1]$. В настоящей статье мы будем говорить, что линейный код с параметрами $[n, k, d]$ оптимален или почти оптимален, если этот код или соответствующий код с параметрами $[n, k, d + 1]$ является наилучшим известным линейным кодом

[1] Работа выполнена при частичной финансовой поддержке Национального фонда естественных наук Китая (номера проектов 61772168, 61572168 и 11871187).

в соответствии с таблицами [2] (или лежит на какой-либо границе для линейных кодов).

В общем случае корректирующая способность циклических кодов может быть не столь хороша, как для других линейных кодов. Однако циклические коды имеют важные применения в системах связи, бытовой электронике и системах хранения информации благодаря наличию эффективных алгоритмов их кодирования и декодирования [3–5]. Поэтому многие исследователи посвящали десятилетия своего труда изучению структуры циклических кодов [6–17]. Имеется несколько подходов к построению всех циклических кодов над конечными полями, а именно порождающие матрицы, порождающие многочлены и порождающие идемпотенты. В последнее десятилетие изучался новый метод построения циклических кодов над $\mathbb{F}_q$ длины n, основанный на порождающем многочлене

$$\frac{x^n-1}{\text{НОД}(S^n(x), x^n-1)}, \tag{1}$$

где

$$S^n(x) = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_q[x],$$

а $s^\infty = (s_i)_{i=0}^\infty$ – последовательность периода n над $\mathbb{F}_q$. Обозначим через C_s циклический код с порождающим многочленом (1). В дальнейшем мы будем называть циклический код C_s кодом, определенным последовательностью s^∞, а последовательность s^∞ – определяющей последовательностью для циклического кода C_s.

Очевидно, что порождающий многочлен кода C_s, определенного последовательностью s^∞, является минимальным многочленом периодической последовательности s^∞, т.е. минимальный многочлен последовательности s^∞ можно использовать как порождающий многочлен циклического кода C_s. В последнее время активно изучалась конструкция циклических кодов, основанная на последовательностях над конечными полями [1,18–21]. В [1,18] с помощью этого подхода были построены некоторые циклические коды, а также сформулированы некоторые открытые проблемы. В дальнейшем многие первоначальные результаты о циклических кодах, получаемых конструкцией, основанной на последовательностях, были улучшены, и были решены некоторые из открытых проблем [20, 21]. В [19] был дан обзор продвижений в этом направлении за последнее десятилетие, а также были поставлены новые открытые проблемы. В настоящей статье мы продолжаем это направление исследований и изучаем три класса циклических кодов, определяемых некоторыми последовательностями с явными многочленами над $\mathbb{F}_{q^m}$. Мы также рассматриваем некоторые из этих открытых проблем.

Статья имеет следующую структуру. В § 2 приводятся некоторые основные обозначения и результаты, относящиеся к q-циклотомическим смежным классам и последовательностям, которые в последующем будут часто использоваться для доказательства основных результатов. Размерности и порождающие многочлены для трех классов циклических кодов, определяемых некоторыми последовательностями с явными многочленами, описываются в § 3. Минимальное расстояние таких циклических кодов также обсуждается в § 3. В частности, построены некоторые оптимальные или почти оптимальные циклические коды. Заключение дано в § 4.

§ 2. Предварительные сведения

Приведем некоторые основные обозначения и результаты, относящиеся к q-циклотомическим смежным классам по модулю n и последовательностям, которые в

дальнейшем будут часто использоваться для доказательства наших основных результатов.

Пусть $n = q^m - 1$ и $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Для любого целого числа s, $0 \leqslant s \leqslant n-1$, определим q-циклотомический смежный класс по модулю n, содержащий s, как

$$C_s = \{s, qs, \ldots, q^{n_s-1}s\} \subset \mathbb{Z}_n,$$

где n_s – наименьшее положительное целое, такое что $q^{n_s}s \equiv s \pmod{n}$, называемое размером смежного класса C_s. Наименьшее целое число, содержащееся в C_s, называется лидером смежного класса C_s. Обозначим множество всех лидеров смежных классов через Γ, тогда $\mathbb{Z}_n = \bigcup\limits_{i\in\Gamma} C_i$. Пусть α – примитивный корень степени n из единицы в некотором расширении поля $\mathbb{F}_q$. Тогда $m_{\alpha^s}(x) = \prod\limits_{j\in C_s}(x - \alpha^j)$ – неприводимый многочлен степени n_s над $\mathbb{F}_q$, являющийся делителем многочлена $x^n - 1$. При этом $x^n - 1 = \prod\limits_{i\in\Gamma} m_{\alpha^i}(x)$ является разложением $x^n - 1$ на неприводимые множители над $\mathbb{F}_q$. Следующие леммы весьма важны для определения размеров некоторых q-циклотомических смежных классов.

Лемма 1. *Для любого целого s, $1 \leqslant s \leqslant q^m - 2$, такого что* НОД$(s, q^m - 1) = 2$ *или* 3, *размер q-циклотомического смежного класса C_s равен m.*

Доказательство. Для случая НОД$(s, q^m - 1) = 2$ доказательство дано в [22]. Для второго случая НОД$(s, q^m - 1) = 3$ доказательство полностью аналогично и поэтому опускается. ▲

Лемма 2 [23]. *q-циклотомический смежный класс по модулю $q^m - 1$ размера ℓ существует тогда и только тогда, когда ℓ делит m.*

Пусть $s^\infty = (s_i)_{i=0}^\infty$ – последовательность периода L над $\mathbb{F}_q$, тогда найдется положительное целое число ℓ, такое что

$$-c_0 s_i = c_1 s_{i-1} + c_2 s_{i-2} + \ldots + c_\ell s_{i-\ell}, \quad i \geqslant \ell,$$

где $c_0 = 1, c_1, \ldots, c_\ell \in \mathbb{F}_q$. Многочлен $c(x) = 1 + c_1 x + \ldots + c_\ell x^\ell$ называется характеристическим многочленом последовательности s^∞. При этом многочлен $M_s(x)$ называется минимальным многочленом последовательности s^∞, если $M_s(x)$ – характеристический многочлен наименьшей степени. Степень минимального многочлена $M_s(x)$ называется линейной сложностью последовательности s^∞ и обозначается через L_s. Более того, известно, что любой характеристический многочлен должен делиться на минимальный многочлен. Для любой периодической последовательности s^∞ над $\mathbb{F}_q$ ее линейную сложность и минимальный многочлен описывает следующая

Лемма 3 [24]. *Пусть s^∞ – последовательность периода L над $\mathbb{F}_q$. Положим*

$$S_L(x) = \sum_{i=0}^{L-1} s_i x^i \in \mathbb{F}_q[x].$$

Тогда минимальный многочлен $M_s(x)$ последовательности s^∞ имеет вид

$$\frac{x^L - 1}{\text{НОД}(S^L(x), x^L - 1)}, \tag{2}$$

а ее линейная сложность L_s равна $L - \deg(\text{НОД}(x^L - 1, S^L(x)))$.

Следующая лемма дает другой способ нахождения линейной сложности и минимального многочлена последовательности s^∞ с периодом q^m-1, который очень важен для доказательства наших основных результатов.

Лемма 4 [24]. *Пусть s^∞ – последовательность с периодом q^m-1 над $\mathbb{F}_q$, имеющая единственное разложение вида*

$$s_t = \sum_{i=0}^{q^m-2} c_i \alpha^{it} \quad \text{для всех } t \geqslant 0,$$

где $c_i \in \mathbb{F}_{q^m}$, а α – образующая группы $\mathbb{F}_{q^m}^*$. Пусть $I = \{i : c_i \neq 0\}$; тогда минимальный многочлен последовательности s^∞ равен

$$M_s(x) = \prod_{i \in I} (1 - \alpha^i x),$$

а ее линейная сложность равна $L_s = |I|$.

§ 3. Циклические коды по некоторым последовательностям над $\mathbb{F}_{q^m}$

В этом параграфе будем рассматривать только специальный тип последовательностей вида

$$s_t = \mathrm{Tr}(f(1+\alpha^t)), \tag{3}$$

где $f(x)$ – некоторый явный многочлен над $\mathbb{F}_{q^m}$, $\mathrm{Tr}(x)$ – функция следа из $\mathbb{F}_{q^m}$ в $\mathbb{F}_q$, а α – примитивный элемент поля $\mathbb{F}_{q^m}$. Код C_s, определяемый одной из последовательностей такого типа, будем для простоты называть кодом по многочлену $f(x)$.

Разумеется, из различных многочленов можно получить огромное количество различных циклических кодов. Цель настоящего параграфа – построить несколько классов циклических кодов по некоторым последовательностям с явными многочленами над $\mathbb{F}_q$.

3.1. Циклические коды по моному $f(x) = x^{q^\ell+2}$. В этом пункте рассматривается код C_s, определяемый мономом $f(x) = x^{q^\ell+2}$ над $\mathbb{F}_{q^m}$, где $m = 2\ell$. Для этого сперва потребуется доказать несколько лемм.

Лемма 5. *Пусть m четно, $m = 2\ell$. Пусть s^∞ – последовательность вида* (3), *где $f(x) = x^{q^\ell+2}$. Пусть $q \neq 2$; тогда линейная сложность L_s последовательности s^∞ равна $2m + N_p(3)m + N_p(4)\ell + N_p(m)$, а ее минимальный многочлен $M_s(x)$ имеет вид*

$$M_s(x) = \begin{cases} m_{\alpha^{-1}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-(q^\ell+2)}}(x), & p = 2, \\ (x-1)^{N_p(m)} m_{\alpha^{-2}}(x) m_{\alpha^{-(q^\ell+1)}}(x) m_{\alpha^{-(q^\ell+2)}}(x), & p = 3, \\ (x-1)^{N_p(m)} m_{\alpha^{-1}}(x) m_{\alpha^{-2}}(x) m_{\alpha^{-(q^\ell+1)}}(x) m_{\alpha^{-(q^\ell+2)}}(x), & p > 3, \end{cases}$$

где $N_p(*) = 0$, если $* \equiv 0 \pmod p$, и $N_p(*) = 1$ в противном случае.

Доказательство. Если $q \neq 2$, то из (3) получаем

$$s_t = \mathrm{Tr}(f(1+\alpha^t)) = \mathrm{Tr}\big((1+\alpha^t)^{q^\ell+2}\big) = \mathrm{Tr}\big((\alpha^t)^{q^\ell+2} + 2(\alpha^t)^{q^\ell+1} + (\alpha^t)^{q^\ell} +$$
$$+ (\alpha^t)^2 + 2(\alpha^t) + 1\big) = \sum_{j=0}^{m-1} (\alpha^t)^{(q^\ell+2)q^j} + 2\sum_{j=0}^{m-1} (\alpha^t)^{(q^\ell+1)q^j} + \sum_{j=0}^{m-1} (\alpha^t)^{(q^\ell)q^j} +$$

$$+\sum_{j=0}^{m-1}(\alpha^t)^{2q^j}+2\sum_{j=0}^{m-1}(\alpha^t)^{q^j}+\mathrm{Tr}(1)=\sum_{j=0}^{m-1}(\alpha^t)^{(q^\ell+2)q^j}+2\sum_{j=0}^{m-1}(\alpha^t)^{(q^\ell+1)q^j}+$$
$$+\sum_{j=0}^{m-1}(\alpha^t)^{2q^j}+3\sum_{j=0}^{m-1}(\alpha^t)^{q^j}+\mathrm{Tr}(1).$$

Заметим, что $(q^\ell+1)\mid(q^m-1)$, поскольку $m=2\ell$. Из леммы 2 легко получить, что размер q-циклотомического смежного класса $C_{q^\ell+1}$ равен ℓ. Имеем

$$\mathrm{НОД}(q^\ell+2,q^m-1)=\mathrm{НОД}(q^\ell+2,(q^\ell+1)(q^\ell-1))=\mathrm{НОД}(q^\ell+2,(q^\ell-1))=$$
$$=\mathrm{НОД}(q^\ell-1+3,(q^\ell-1))\leqslant 3,$$

так как $m=2\ell$ и $\mathrm{НОД}(q^\ell+2,(q^\ell+1))=1$. Тогда из леммы 1 получаем $|C_{q^\ell+2}|=m$. Очевидно, что C_1, C_2, $C_{q^\ell+1}$ и $C_{q^\ell+2}$ попарно различны. Поэтому s_t можно упростить следующим образом:

$$s_t=\sum_{j=0}^{m-1}(\alpha^t)^{(q^\ell+2)q^j}+4\sum_{j=0}^{\ell-1}(\alpha^t)^{(q^\ell+1)q^j}+\sum_{j=0}^{m-1}(\alpha^t)^{2q^j}+3\sum_{j=0}^{m-1}(\alpha^t)^{q^j}+\mathrm{Tr}(1).$$

Более того, нетрудно проверить, что $N_p(m)=N_p(4)=0$, если $p=2$, $N_p(3)=0$ и $N_p(4)=1$, если $p=3$, и $N_p(3)=N_p(4)=1$, если $p>3$. Требуемые результаты о линейной сложности L_s и минимальном многочлене $M_s(x)$ теперь следуют из леммы 4. ▲

Лемма 6. *Если $q=2$, то линейная сложность L_s последовательности s^∞ из леммы 5 равна m, а ее минимальный многочлен $M_s(x)$ имеет вид*

$$M_s(x)=m_{\alpha^{-(2^{\ell-1}+1)}}(x).$$

Доказательство. Если $q=2$, то из (3) получаем

$$s_t=\mathrm{Tr}\big((1+\alpha^t)^{2^\ell+2}\big)=\mathrm{Tr}\big((\alpha^t)^{2^\ell+2}+2(\alpha^t)^{2^\ell+1}+(\alpha^t)^{2^\ell}+(\alpha^t)^2+2(\alpha^t)+1\big)=$$
$$=\mathrm{Tr}\big((\alpha^t)^{2^\ell+2}\big)=\mathrm{Tr}\big((\alpha^t)^{2^{\ell-1}+1}\big).$$

Заметим, что

$$\mathrm{НОД}(2^{\ell-1}+1,2^{2\ell}-1)=\begin{cases}1, & \text{если } \dfrac{2\ell}{\mathrm{НОД}(\ell-1,2\ell)} \text{ нечетно},\\ 3, & \text{если } \dfrac{2\ell}{\mathrm{НОД}(\ell-1,2\ell)} \text{ четно}.\end{cases}$$

Таким образом,

$$\mathrm{НОД}(2^{\ell-1}+1,2^{2\ell}-1)=\begin{cases}1, & \text{если } \ell \text{ нечетно},\\ 3, & \text{если } \ell \text{ четно}.\end{cases}$$

По лемме 1 получаем, что размер смежного класса $C_{2^{\ell-1}+1}$ равен m. Требуемые результаты о линейной сложности L_s и минимальном многочлене $M_s(x)$ теперь следуют из леммы 4. ▲

Итак, параметры и порождающий многочлен циклического кода C_s, определяемого последовательностью s^∞, описывает следующая

Теорема 1. *Пусть C_s – циклический код, определяемый последовательностью s^∞ из леммы 5. Тогда справедливы следующие утверждения*:

(1) *При $q \neq 2$ код C_s имеет параметры $[n, n-2m-N_p(3)m-N_p(4)\ell-N_p(m), d]$ и порождающий многочлен $M_s(x)$, описанный в лемме 5, где*

$$\begin{cases} 3 \leqslant d \leqslant 6, & p = 2 \text{ или } 3, \\ 4 \leqslant d \leqslant 8, & p > 3. \end{cases}$$

(2) *При $q = 2$ код C_s имеет параметры $[n, n-m, d]$ и порождающий многочлен $M_s(x)$, описанный в лемме 6, где*

$$d = \begin{cases} 2, & \text{если } \ell \text{ четно}, \\ 3, & \text{если } \ell \text{ нечетно}. \end{cases}$$

Доказательство. (1) Очевидно, требуется лишь доказать границы на минимальное расстояние Хэмминга кода C_s. Заметим, что коды, порождаемые многочленом $M_s(x)$ и взаимным к нему многочленом, имеют одинаковое распределение весов. Легко видеть, что многочлен, взаимный к $M_s(x)$, имеет корни α и α^2, когда $q \neq 2$ и $p = 2$. В этом случае $d \geqslant 3$ согласно границе БЧХ. Аналогично получаем $d \geqslant 3$, когда $p = 3$, и $d \geqslant 4$, когда $p = 2$. Теперь оценим минимальное расстояние сверху, используя границу Хэмминга и размерность этих кодов.

(2) При $q = 2$ пусть C_s^* – циклический код, порождаемый многочленом, взаимным к $M_s(x)$. Ясно, что минимальное расстояние d кода C_s^* не может быть равно 1. Из границы Хэмминга и размерности кода получаем, что $d \leqslant 4$. Из леммы 5 работы [25] известно, что минимальное расстояние d кода C_s^* не может быть равно 4. Таким образом, $2 \leqslant d \leqslant 3$. Если ℓ четно, то НОД$(2^{\ell-1}+1, 2^{2\ell}-1) = 3$. Положим $D = \dfrac{\ell^{2\ell}-1}{3}$. Далее, легко видеть, что $m_{\alpha^{2^{\ell-1}+1}}(x) \mid (x^D-1)$, поскольку все корни многочлена $m_{\alpha^{2^{\ell-1}+1}}(x)$ являются корнями многочлена x^D-1. Таким образом, $d = 2$. В противном случае легко видеть, что кодовых слов веса Хэмминга 2 не существует, если НОД$(2^{\ell-1}+1, 2^{2\ell}-1) = 1$. Таким образом, $d = 3$, если ℓ нечетно. ▲

Замечание 1. Следует отметить, что подкласс двоичных циклических кодов C_s, построенных по моному $f(x) = x^{2^\ell+2}$ над $\mathbb{F}_{2^m}$, оптимален, когда ℓ нечетно, и почти оптимален, когда ℓ четно, где $m = 2\ell$. Как правило, двойственный код циклического кода C_s также оптимален, когда ℓ нечетно, что показано в следующей таблице ($q = 2$):

ℓ	Код C_s	Двойственный код	Оптимальность / почти оптимальность
1	$[3, 1, 3]$	$[3, 2, 2]$	Оба оптимальны (МДР)
2	$[15, 11, 2]$	$[15, 4, 6]$	C_s почти оптимален
3	$[63, 57, 3]$	$[63, 6, 32]$	Оба оптимальны
4	$[255, 247, 2]$	$[255, 8, 120]$	C_s почти оптимален
5	$[1023, 1013, 3]$	$[1023, 10, 512]$	Оба оптимальны
6	$[4095, 4083, 2]$	$[4095, 12, 2016]$	C_s почти оптимален
⋮	⋮	⋮	⋮

Пример 1. Пусть $(\ell, m, q) = (1, 2, 4)$, ω – примитивный элемент поля $\mathbb{F}_4$, и пусть $\mathbb{F}_{4^2} = \mathbb{F}_4[\alpha]$, где $\alpha^2 + \alpha + \omega = 0$. Тогда порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^6 + \omega^2 x^5 + \omega^2 x^4 + x^3 + x^2 + \omega x + 1,$$

а C_s является четверичным $[15, 9, 5]$-кодом. Его двойственный код – четверичный циклический $[15, 6, 8]$-код. Оба кода почти оптимальны.

Пример 2. Пусть $(\ell, m, q) = (1, 2, 8)$, ω – примитивный элемент поля $\mathbb{F}_8$, и пусть $\mathbb{F}_{8^2} = \mathbb{F}_8[\alpha]$, где $\alpha^2 + \omega\alpha + \omega = 0$. Тогда порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^6 + w^6x^5 + w^6x^4 + w^4x^3 + w^4x^2 + w^2x + w,$$

а C_s является циклическим $[63, 57, 3]$-кодом над $\mathbb{F}_8$. Его двойственный код – циклический $[63, 6, 48]$-код над $\mathbb{F}_8$. Оба кода почти оптимальны.

Пример 3. Пусть $(\ell, m, q) = (1, 2, 7)$, а α – примитивный элемент поля $\mathbb{F}_{7^2}$, такой что $\alpha^2 + 6\alpha + 3 = 0$. Тогда порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^8 + 5x^7 + 4x^6 + 3x^5 + 6x^4 + 5x^3 + 6x + 5,$$

а C_s является циклическим $[48, 40, 5]$-кодом над $\mathbb{F}_7$. Этот циклический код почти оптимален. Но его двойственный код – оптимальный циклический $[48, 8, 33]$-код над $\mathbb{F}_7$.

3.2. Циклические коды по моному $f(x) = x^{q^h-1}$. В этом пункте рассмотрим циклический код, определяемый над $\mathbb{F}_{q^m}$ мономом вида $f(x) = x^{q^h-1}$, где h – положительное целое число. Для любого положительного целого $h \geqslant m$ пусть $h = mk+\ell$, где k, ℓ – некоторые явные положительные целые числа и $\ell \leqslant m-1$. Ясно, что $f(x) = x^{q^h-1} = x^{q^\ell-1}$. В этом пункте рассматривается случай $h \leqslant m-1$.

Прежде чем сформулировать и доказать основной результат, введем некоторые новые обозначения, которые понадобятся для дальнейшего. Пусть ℓ_s – размер q-циклотомического смежного класса C_s, содержащего элемент $s \in \Gamma$. Тогда существует единственное целое h_s, такое что $\ell_s h_s = m$. Определим q-адическое разложение числа s как $s = i_0+i_1q+\ldots+i_{m-1}q^{m-1}$, где $0 \leqslant i_0, i_1, \ldots, i_{m-1} \leqslant q-1$, и будем представлять его последовательностью вида $s = (i_0, i_1, i_2, \ldots, i_{m-1})$. Очевидно, что для любого элемента $i \in C_s$ его q-адическое разложение является некоторым сдвигом последовательности $s = (i_0, i_1, i_2, \ldots, i_{m-1})$. В последовательности $s = (i_0, i_1, i_2, \ldots, i_{m-1})$ любые ℓ подряд идущих нулей будем называть 0-серией длины ℓ. Обозначим все 0-серии в $s = (i_0, i_1, i_2, \ldots, i_{m-1})$ через $A_1^s, A_2^s, \ldots, A_{d_s}^s$. Кроме того, пусть m_i^s – длина 0-серии A_i^s для любого $1 \leqslant i \leqslant d_s$. Пусть $m_{s,k,u} = |\{t : i_t = k \text{ и } 0 \leqslant t \leqslant u\}|$ для любых положительных целых k, u, таких что $0 \leqslant k \leqslant q-1$ и $0 \leqslant u \leqslant m-1$. Теперь зададим разложение функции

$$\begin{aligned} f(\alpha^t + 1) &= (\alpha^t + 1)^{q^h-1} = (\alpha^t + 1)^{(q-1)\sum\limits_{i=0}^{h-1} q^i} = \\ &= (\alpha^{tq^0} + 1)^{q-1}(\alpha^{tq^1} + 1)^{q-1} \ldots (\alpha^{tq^{h-1}} + 1)^{q-1} = \\ &= \sum_{0 \leqslant i_0, i_1, \ldots, i_{h-1} \leqslant q-1} \binom{q-1}{i_0} \ldots \binom{q-1}{i_{h-1}} (\alpha^t)^{i_0+i_1q+i_2q^2+\ldots+i_{h-1}q^{h-1}}. \end{aligned}$$

Положим $\Gamma' = \{s \in \Gamma : m_{s,0,m-1} + m_{s,1,h-1} + \ldots + m_{s,q-1,h-1} = m\}$, а также $C'_s = \{i \in C_s : i < q^h\}$ для любого $s \in \Gamma'$. Очевидно, $0 \in \Gamma'$. Кроме того, для любых $s \in \Gamma'$ и $i \in C'_s$ положим

$$B_{s,i} = \binom{q-1}{i_0}\binom{q-1}{i_1}\binom{q-1}{i_{h-1}}.$$

Заметим, что $B_{s,i} = B_{s,s}$ (обозначим эту величину просто через B_s) для любого $i \in C'_s$.

Таким образом, получаем

$$f(\alpha^t+1)=\sum_{s\in\Gamma'}\sum_{i\in C'_s}\binom{q-1}{i_0}\binom{q-1}{i_1}\binom{q-1}{i_{h-1}}(\alpha^t)^i=\sum_{s\in\Gamma'}\sum_{i\in C'_s}B_{s,i}(\alpha^t)^i=$$
$$=\sum_{s\in\Gamma'}\sum_{i\in C'_s}B_s(\alpha^t)^i=\sum_{s\in\Gamma'}B_s\sum_{i\in C'_s}(\alpha^t)^i.$$

Для любого $s\in\Gamma'\setminus\{0\}$ определим N'_s следующим образом:

$$N'_s=\sum_{\substack{1\leqslant i\leqslant d_s\\ m_i^s\geqslant m-h}}(m_i^s-m+h+1).$$

Нетрудно доказать следующие леммы.

Лемма 7. *Пусть B_s определено, как и выше; тогда* $\text{НОД}(B_s,p)=1$.

Доказательство. Пусть $q=p^a$, тогда p-адическим разложением $q-1$ является

$$q-1=(p-1)\sum_{j=0}^{a-1}p^j.$$

Для любого $0\leqslant i\leqslant q-1$ пусть $i=\sum\limits_{j=0}^{a-1}i_jp^j$, где $0\leqslant i_0,i_1,\ldots,i_{a-1}\leqslant p-1$. Согласно теореме Люка [26]

$$\binom{q-1}{i}=\binom{p-1}{i_0}\binom{p-1}{i_1}\binom{p-1}{i_{a-1}}\mod p.$$

Заметим, что $\text{НОД}\left(\binom{p-1}{i_j},p\right)=1$, поскольку p – простое. Таким образом,

$$\text{НОД}\left(\binom{q-1}{i},p\right)=1.\quad\blacktriangle$$

Лемма 8. *Пусть s^∞ – последовательность вида* (3) *с мономом $f(x)=x^{q^h-1}$ над $\mathbb{F}_{q^m}$, где $h\leqslant m-1$. Тогда линейная сложность L_s и минимальный многочлен $M_s(x)$ последовательности s^∞ имеют вид*

$$L_s=\sum_{s\in\Gamma'\setminus\{0\}}N_p(N'_s)\ell_s+N_p(m)$$

и

$$M_s(x)=(x-1)^{N_p(m)}\prod_{s\in\Gamma'\setminus\{0\}}m_{\alpha^{-s}}(x)^{N_p(N'_s)},$$

где $N_p(*)=0$, если $*\equiv 0\pmod p$, и $N_p(*)=1$ в противном случае.

Доказательство. Объединяя предыдущие рассуждения с формулой (3), получаем

$$s_t=\text{Tr}(f(\alpha^t+1))=\text{Tr}\left(\sum_{s\in\Gamma'}B_s\sum_{i\in C'_s}(\alpha^t)^i\right)=\sum_{s\in\Gamma'}B_s\sum_{i\in C'_s}\text{Tr}((\alpha^t)^i)=$$

$$= \mathrm{Tr}(1) + \sum_{s\in\Gamma'\setminus\{0\}} \frac{B_s}{h_s} \sum_{\substack{1\leqslant i\leqslant d_s\\ m_i^s\geqslant m-h}} (m_i^s - m + h + 1)\,\mathrm{Tr}((\alpha^t)^s) =$$

$$= \mathrm{Tr}(1) + \sum_{s\in\Gamma'\setminus\{0\}} \frac{B_s}{h_s} \sum_{\substack{1\leqslant i\leqslant d_s\\ m_i^s\geqslant m-h}} (m_i^s - m + h + 1) \sum_{u=0}^{m-1} (\alpha^t)^{sq^u} =$$

$$= \mathrm{Tr}(1) + \sum_{s\in\Gamma'\setminus\{0\}} \frac{B_s}{h_s} \sum_{\substack{1\leqslant i\leqslant d_s\\ m_i^s\geqslant m-h}} (m_i^s - m + h + 1) h_s \sum_{i\in C_s} (\alpha^t)^i =$$

$$= \mathrm{Tr}(1) + \sum_{s\in\Gamma'\setminus\{0\}} B_s \sum_{\substack{1\leqslant i\leqslant d_s\\ m_i^s\geqslant m-h}} (m_i^s - m + h + 1) \sum_{i\in C_s} (\alpha^t)^i =$$

$$= \mathrm{Tr}(1) + \sum_{s\in\Gamma'\setminus\{0\}} B_s N_s' \sum_{i\in C_s} (\alpha^t)^i.$$

Так как НОД$(B_s, p) = 1$, то $N_p(B_s N_s') = N_p(N_s')$. Поэтому требуемые результаты о линейной сложности L_s и минимальном многочлене $M_s(x)$ теперь вытекают из леммы 4. ▲

Итак, получена следующая теорема, описывающая параметры и порождающий многочлен циклического кода C_s, определяемого последовательностью s^∞.

Теорема 2. *Пусть C_s – циклический код, определяемый последовательностью s^∞ из леммы 8. Тогда C_s имеет параметры $[n, n - L_s, d]$ и порождающий многочлен $M_s(x)$, где L_s и $M_s(x)$ указаны в лемме 7.*

Следствие 1. *Если $h = m - 1$ и $m \leqslant p$, то циклический код C_s из теоремы 2 имеет параметры $[n, n - L_s, d]$ и порождающий многочлен*

$$M_s(x) = \begin{cases} \prod\limits_{s\in\Gamma'} m_{\alpha^{-s}}(x), & m < p,\\ \prod\limits_{s\in\Gamma'\setminus\{0\}} m_{\alpha^{-s}}(x), & m = p, \end{cases}$$

где

$$L_s = \begin{cases} q^m - (q-1)^m, & m < p,\\ q^m - (q-1)^m - 1, & m = p, \end{cases}$$

и

$$\begin{cases} \dfrac{q^m - 1}{q-1} + 1 \leqslant d \leqslant q^m - (q-1)^m + 1, & m < p,\\ \dfrac{q^m - 1}{q-1} \leqslant d \leqslant q^m - (q-1)^m, & m = p. \end{cases}$$

Доказательство. Для любого положительного целого $i < p$ имеем $N_p(i) = 1$, поскольку НОД$(i, p) = 1$. Заметим, что

$$N_s' = \sum_{\substack{1\leqslant i\leqslant d_s\\ m_i^s\geqslant m-h}} (m_i^s - m + h + 1) \leqslant m - 1 < p \quad \text{для любого } s \in \Gamma' \setminus \{0\}.$$

Поэтому $N_p(N_s') = 1$. Более того, $N_p(m) = 1$, если $m < p$, и $N_p(m) = 0$, если $m = p$. По лемме 8 получаем параметры $[n, n - L_s, d]$ и порождающий многочлен $M_s(x)$

кода C_s, где $L_s = \sum\limits_{s\in\Gamma'\setminus\{0\}} \ell_s + N_p(m)$. Кроме того, $\sum\limits_{s\in\Gamma'\setminus\{0\}} \ell_s = q^m-(q-1)^m-1$, так как $h = m-1$. Следовательно, $L_s = q^m-(q-1)^m$, если $m < p$, и $L_s = q^m-(q-1)^m-1$, если $m = p$. Очевидно, что $\alpha^0, \alpha^1, \ldots, \alpha^{q^{m-1}}, \ldots, \alpha^{q^{m-1}+q^{m-2}+\ldots+q^2+q}$ – корни многочлена, взаимного к $M_s(x)$, когда $m < p$. Таким образом, $\dfrac{q^m-1}{q-1} + 1 \leqslant d$ согласно границе БЧХ. Оценку сверху для d можно получить из границы Синглтона. Аналогично получаются оценки для d при $m = p$. ▲

Рассмотрим случай $q = 2$. Из теоремы 2 немедленно получаем

Следствие 2. *Пусть $q = 2$. Тогда циклический код C_s из теоремы 2 имеет параметры $[2^m-1, 2^m-1-L_s, d]$ и порождающий многочлен $M_s(x)$, где*

$$L_s = \sum_{s\in\Gamma'\setminus\{0\}} N_2(N'_s)\ell_s + N_2(m),$$
$$M_s(x) = (x-1)^{N_2(m)} \prod_{\substack{s\in\Gamma'\setminus\{0\}\\ N_2(N'_s)=1}} m_{\alpha^{-s}}(x)$$

и

$$\begin{cases} d \geqslant 2^{h-2}+2, & m \text{ нечетно и } 2 < h \leqslant \left\lceil \dfrac{m}{2} \right\rceil, \\ d \geqslant 2^{h-2}+1, & m \text{ четно и } 2 < h \leqslant \left\lceil \dfrac{m}{2} \right\rceil. \end{cases}$$

Замечание 2. Пусть при этом $q = 2$ и $1 \leqslant h \leqslant \lceil m/2 \rceil$. Для этого подслучая в [1] исследован двоичный циклический код C_s, определяемый последовательностью s^∞ вида (3). Покажем, что наши результаты равносильны результатам из [1, теорема 12]. Согласно [1]

$$M_s(x) = (x-1)^{N_2(m)} \prod_{\substack{1\leqslant 2j+1\leqslant 2^h-1\\ \varkappa^{(h)}_{2j+1}=1}} m_{\alpha^{-(2j+1)}}(x).$$

Так как $q = 2$ и $h \leqslant \lceil m/2 \rceil$, то нетрудно видеть, что

$$i = i_0 + i_1 2 + \ldots + i_{h-1}2^{h-1} \in \Gamma' \setminus \{0\}$$

тогда и только тогда, когда $i_0 = 1$. Таким образом, любое целое i, $1 \leqslant i \leqslant 2^h-1$, вида $i = 2j+1$ принадлежит $\Gamma' \setminus \{0\}$, и любой элемент $i \in \Gamma' \setminus \{0\}$ имеет вид $2j+1$, т.е.

$$\Gamma' \setminus \{0\} = \{2j+1 :\ 1 \leqslant 2j+1 \leqslant 2^h-1\}.$$

Кроме того, согласно определениям величин $\varkappa^{(h)}_{2j+1}$ (см. [1]) и $N_2(N'_s)$ нетрудно проверить, что $\varkappa^{(h)}_{2j+1} = N_2(N'_s)$, когда $s = 2j+1$. Таким образом,

$$M_s(x) = (x-1)^{N_2(m)} \prod_{\substack{1\leqslant 2j+1\leqslant 2^h-1\\ \varkappa^{(h)}_{2j+1}=1}} m_{\alpha^{-(2j+1)}}(x) = (x-1)^{N_2(m)} \prod_{\substack{s\in\Gamma'\setminus\{0\}\\ N_2(N'_s)=1}} m_{\alpha^{-s}}(x).$$

Пример 4. Пусть $(q, m, h) = (3, 4, 1)$, а α – примитивный элемент поля $\mathbb{F}_{3^4}$, такой что $\alpha^4 + 2\alpha^3 + 2 = 0$. Тогда $\Gamma' = \{0, 1, 2\}$. Легко убедиться, что $N_3(N'_s) = 1$,

когда $s \in \Gamma' \setminus \{0\}$. При этом порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^9 + 2x^8 + x^7 + 2x^6 + x^4 + x^2 + 1,$$

и C_s является троичным циклическим $[80, 71, 5]$-кодом. Его двойственный код – троичный циклический $[80, 9, 47]$-код. Оба кода оптимальны.

Пример 5. Пусть $(q, m, h) = (3, 4, 2)$, а α – примитивный элемент поля $\mathbb{F}_{3^4}$, такой что $\alpha^4 + 2\alpha^3 + 2 = 0$. Тогда $\Gamma' = \{0, 1, 2, 4, 5, 7, 8\}$. Нетрудно убедиться, что $N_3(N'_s) = 1$, когда $s \in \Gamma' \setminus \{0\}$. При этом порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^{25} + x^{24} + 2x^{23} + 2x^{22} + x^{21} + 2x^{18} + x^{15} + 2x^{11} + 2x^{10} + x^9 + x^7 + \\ + 2x^5 + 2x^4 + x^3 + x^2 + x + 1,$$

и C_s является оптимальным троичным циклическим $[80, 55, 11]$-кодом. Его двойственный код – циклический $[55, 25, 24]$-код.

Пример 6. Пусть $(q, m, h) = (5, 3, 1)$, а α – примитивный элемент поля $\mathbb{F}_{5^3}$, такой что $\alpha^3 + 3\alpha + 3 = 0$. Тогда $\Gamma' = \{0, 1, 2, 3, 4\}$. Нетрудно проверить, что $N_5(N'_s) = 1$, когда $s \in \Gamma' \setminus \{0\}$. При этом порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^{13} + 2x^{12} + 4x^{11} + 2x^{10} + 4x^9 + x^8 + 4x^7 + 2x^5 + x^3 + 2x^2 + x + 1,$$

и C_s является циклическим $[124, 111, 7]$-кодом над $\mathbb{F}_5$. Его двойственный код – циклический $[124, 13, 82]$-код. Оба кода оптимальны.

3.3. Циклические коды по моному $f(x) = x^{q^{(3m-1)/4}+(q^{(m-1)/2}-1)/(q-1)}$. В этом пункте будем изучать циклический код C_s, определяемый по моному

$$f(x) = x^{q^{(3m-1)/4}+(q^{(m-1)/2}-1)/(q-1)}$$

над $\mathbb{F}_{q^m}$, где m – положительное целое число, такое что $m \equiv 3 \pmod 4$. Тем самым, существует целое k, такое что $m = 4k + 3$. С этой целью сперва рассмотрим разложение функции

$$f(\alpha^t + 1) = (\alpha^t + 1)^{q^{(3m-1)/4}+(q^{(m-1)/2}-1)/(q-1)} = (\alpha^t + 1)^{q^{3k+2}+(q^{2k+1}-1)/(q-1)} = \\ = (\alpha^t + 1)^{\sum_{i=0}^{2k} q^i + q^{3k+2}} = (\alpha^{tq^0} + 1)(\alpha^{tq^1} + 1) \dots (\alpha^{tq^{2k}} + 1)(\alpha^{tq^{3k+2}} + 1) = \\ = \sum_{0 \leqslant i_0, \dots, i_{2k}, i_{3k+2} \leqslant 1} (\alpha^t)^{i_0 + i_1 q + i_2 q^2 + \dots + i_{2k} q^{2k} + i_{3k+2} q^{3k+2}} = \\ = \sum_{0 \leqslant i_0, \dots, i_{2k} \leqslant 1} (\alpha^t)^{i_0 + i_1 q + i_2 q^2 + \dots + i_{2k} q^{2k}} + \sum_{0 \leqslant i_0, \dots, i_{2k} \leqslant 1} (\alpha^t)^{i_0 + i_1 q + i_2 q^2 + \dots + i_{2k} q^{2k} + q^{3k+2}}.$$

Всюду далее будем использовать обозначения

$$A = \{i : \ i = i_0 + i_1 q + i_2 q^2 + \dots + i_{2k} q^{2k}, \ 0 \leqslant i_0, \dots, i_{2k} \leqslant 1\},$$
$$B = q^{3k+2} + A = \{j : \ j = i + q^{3k+2} \text{ и } i \in A\}.$$

Тогда любые элементы $i \in A$ и $j \in B$ можно представить в виде последовательностей $i = (\underbrace{\star, \dots, \star}_{2k+1}, \underbrace{0, \dots, 0}_{2k+2})$ и $j = (\underbrace{\star, \dots, \star}_{2k+1}, \underbrace{0, \dots, 0}_{k+1}, 1, \underbrace{0, \dots, 0}_{k})$ соответственно, где $\star \in \{0, 1\}$. На протяжении этого пункта всегда будем считать, что $\star \in \{0, 1\}$, если не указано обратное. Что более важно, лидеры смежных классов всех элементов множества A

образуют множество

$$\overline{A} = \{i \in A :\ i = (1, \underbrace{\star, \ldots, \star}_{2k}, \underbrace{0, \ldots, 0}_{2k+2})\}.$$

Лемма 9. *Для любого $i \in A$ смежный класс C_i имеет размер $\ell_i = |C_i| = m = 4k+3$.*

Доказательство. Заметим, что $i < q^{2k+1}$; тогда $iq^t \leqslant q^m - 1$ для любого t, $0 \leqslant t \leqslant 2k+2$. Это означает, что $|C_i| > 2k+2 > \frac{m}{2}$. По лемме 2 получаем $\ell_i = |C_i| = m$. ▲

Лемма 10. *Пусть $j \in B$. Тогда $|C_j| = m = 4k+3$, если* НОД$(3,k) = 1$, *а если $k = 3k'$, то $|C_j| = \frac{m}{3}$ тогда и только тогда, когда $j = q^{k'} + q^{5k'+1} + q^{9k'+2}$, а в противном случае $|C_j| = m$.*

Доказательство. Замети, что $j < q^{3k+2}$, поэтому $jq^t \leqslant q^m - 1$ для любого $0 \leqslant t \leqslant k+1$. Тогда $|C_j| > k+1 = \frac{m+1}{4} > \frac{m}{4}$. Если НОД$(m,2) = 1$ и НОД$(m,3) = 1$, то C_j должен иметь размер m согласно лемме 2. Если $k = 3k'$, то размер C_j должен быть либо m, либо $\frac{m}{3}$. Предположим, что $|C_j| = \frac{m}{3}$, тогда представление j в виде последовательности можно разбить на три части равной длины, причем все три части должны быть одинаковы. Замечая, что $\frac{m}{3} = k + \frac{k}{3} + 1$, отсюда легко вывести, что каждая часть имеет вид $(\underbrace{0, \ldots, 0}_{\frac{k}{3}}, 1, \underbrace{0, \ldots, 0}_{k})$. Таким образом,

$$j = (\underbrace{0, \ldots, 0}_{\frac{k}{3}}, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{\frac{k}{3}}, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{\frac{k}{3}}, 1, \underbrace{0, \ldots, 0}_{k}),$$

т.е. $j = q^{k'} + q^{5k'+1} + q^{9k'+2}$. Пусть теперь $j = q^{k'} + q^{5k'+1} + q^{9k'+2}$, тогда ясно, что $|C_j| = \frac{m}{3}$. На этом доказательство завершается. ▲

Поскольку случаи $k = 0$ и 1 очевидны, в дальнейшем будем предполагать, что $k \geqslant 2$. Положим

$$B_1 = \{j \in B :\ j = (\underbrace{\star, \ldots, \star}_{k}, \underbrace{0, \ldots, 0}_{k+1}, \underbrace{0, \ldots, 0}_{k+1}, 1, \underbrace{0, \ldots, 0}_{k})\},$$

$$B_2 = \{j \in B :\ j = (\underbrace{0, \ldots, 0}_{k+2}, \underbrace{\star, \ldots, \star}_{k-1}, \underbrace{0, \ldots, 0}_{k+1}, 1, \underbrace{0, \ldots, 0}_{k})\}.$$

Разумеется, для любого элемента j множества B_1 или B_2 должен существовать некоторый лидер смежного класса $i \in \overline{A}$, такой что $j \in C_i$. Более того, множество лидеров смежных классов всех элементов множества B_1 (или B_2) имеет вид

$$\overline{B}_1 = \{1, \underbrace{0, \ldots, 0}_{k}, \underbrace{\star, \ldots, \star}_{k}, \underbrace{0, \ldots, 0}_{2k+2})\}$$

$$(\text{или } \overline{B}_2 = \{1, \underbrace{\star, \ldots, \star}_{k-t-2}, \underbrace{0, \ldots, 0}_{k+1}, 1, \underbrace{0, \ldots, 0}_{2k+2}, \underbrace{0, \ldots, 0}_{t},\ 0 \leqslant t \leqslant k-2)\} \cup \{1\}).$$

Таким образом, можно сформулировать следующие леммы.

Лемма 11. *Для любого $j \in B$ существует некоторый элемент $i \in A$, такой что $C_i \cap C_j \neq \varnothing$ тогда и только тогда, когда $j \in B_1$ или B_2.*

Лемма 12. *Для любых $j_1 \in B_1$ и $j_2 \in B_2$ справедливы следующие два утверждения*:

(1) *$j_1 = j_2$ тогда и только тогда, когда* $j_1 = j_2 = (\underbrace{0,\dots,0}_{3k+2},1,\underbrace{0,\dots,0}_{k})$;

(2) *$C_{j_1} = C_{j_2}$ $(j_1 \neq j_2)$ тогда и только тогда, когда*

$$j_1 = (\underbrace{0,\dots,0}_{k-t},1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{k+t+1},1,\underbrace{0,\dots,0}_{k})$$

и

$$j_2 = (\underbrace{0,\dots,0}_{k+t+1},1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{k-t},1,\underbrace{0,\dots,0}_{k}),$$

где $1 \leqslant t \leqslant k-1$.

Доказательство. Первое утверждение тривиально. Докажем второе. Если $C_{j_1} = C_{j_2}$ $(j_1 \neq j_2)$, то $j_2 \in C_{j_1}$, т.е. представление j_2 в виде последовательности является некоторым сдвигом

$$j_1 = (\underbrace{\star,\dots,\star}_{k},\underbrace{0,\dots,0}_{k+1},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{k}).$$

Очевидно, что r-кратный сдвиг j_1 не принадлежит B_2, когда $0 \leqslant r \leqslant 2k+2$ или $3k+2 \leqslant r \leqslant m$. Таким образом, считаем, что $(t+2k+2)$-кратный сдвиг j_1 равен j_2, где $1 \leqslant t \leqslant k-1$. Тогда

$$j_2 = (\underbrace{0,\dots,0}_{t},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{k},\underbrace{\star,\dots,\star}_{k},\underbrace{0,\dots,0}_{k+1-t}).$$

Поскольку $j_2 \in B_2$, получаем, что

$$j_2 = (\underbrace{0,\dots,0}_{t},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{k-t},1,\underbrace{0,\dots,0}_{k}).$$

Следовательно,

$$j_1 = (\underbrace{0,\dots,0}_{k-t},1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{t},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{k}).$$

В обратную сторону утверждение очевидно. ▲

Для любого $j \in B$ положим $C'_j = \{j' : j' \in C_j \text{ и } j' \in B\}$, а через ℓ'_j обозначим мощность C'_j. Более точно, будем считать, что $C'_j = \{j, j_1, \dots, j_t\}$ и $j \to j_1 \to \dots \to j_t \to j$. Поскольку представление в виде последовательности для каждого элемента C'_j имеет вид $(\underbrace{\star,\dots,\star}_{2k+1},\underbrace{0,\dots,0}_{k},0,1,\underbrace{0,\dots,0}_{k})$, то для каждого элемента C'_j требуется не менее $k+2$ сдвигов для получения следующего элемента. Тогда общее число сдвигов не меньше $(t+1)(k+2)$. Если $\ell_j = m$, то $(t+1)(k+2) \leqslant m = 4k+3$. Следовательно, $t \leqslant 2$, т.е. $\ell'_j \leqslant 3$. Если $\ell_j = \dfrac{m}{3}$, то $(t+1)(k+2) \leqslant \ell_j = \dfrac{4k+3}{3}$. Значит, $t \leqslant 1$, т.е. $\ell'_j = 1$.

Пусть

$$B'_1 = \{j \in B_1 : j = (\underbrace{0,\dots,0}_{k-t},1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{k+t+1},1,\underbrace{0,\dots,0}_{k})\},$$

$$B'_2 = \{j \in B_2 :\ j = (\underbrace{0,\dots,0}_{k+t+1}, 1, \underbrace{0,\dots,0}_{k}, \underbrace{0,\dots,0}_{k-t}, 1, \underbrace{0,\dots,0}_{k})\},$$

где $1 \leqslant t \leqslant k-1$. Лидеры смежных классов всех элементов из B'_1 (или B'_2) образуют множество

$$\overline{B}'_1 = \{j :\ j = (1, \underbrace{0,\dots,0}_{2k-t}, 1, \underbrace{0,\dots,0}_{2k+t+1}),\ 1 \leqslant t \leqslant k-1\}.$$

Согласно доказательству леммы 12 имеем

$$B'_1 \cup B'_2 = \bigcup_{j \in B'_1} C'_j = \bigcup_{j \in B'_2} C'_j.$$

Положим

$$D = \{j \in B :\ j = (\underbrace{\star,\dots,\star}_{k-t-1}, \underbrace{0,\dots,0}_{k+1}, 1, \underbrace{0,\dots,0}_{k}, \underbrace{0,\dots,0}_{t}, 0, 1, \underbrace{0,\dots,0}_{k})\},$$

где $0 \leqslant t \leqslant k-1$, и

$$O = \{j \in B :\ j = (\underbrace{0,\dots,0}_{2k-t}, 1, \underbrace{0,\dots,0}_{k}, \underbrace{\star,\dots,\star}_{t-k}, \underbrace{0,\dots,0}_{k+1}, 1, \underbrace{0,\dots,0}_{k})\},$$

где $k \leqslant t \leqslant 2k-1$. Кроме того, при $k \geqslant 3$ положим

$$D' = \{j' \in D :\ j' = (0, \underbrace{\star,\dots,\star}_{k-t-2}, \underbrace{0,\dots,0}_{k+1}, 1, \underbrace{0,\dots,0}_{t}, \underbrace{0,\dots,0}_{k+1}, 1, \underbrace{0,\dots,0}_{k})\},$$

где $0 \leqslant t \leqslant k-3$, и

$$O' = \{j' \in O :\ j' = (\underbrace{0,\dots,0}_{2k-t}, 1, \underbrace{0,\dots,0}_{k+1}, \underbrace{\star,\dots,\star}_{t-k-1}, \underbrace{0,\dots,0}_{k+1}, 1, \underbrace{0,\dots,0}_{k})\},$$

где $k+2 \leqslant t \leqslant 2k-1$. В последовательностях из множеств D' и O' имеется один и только один элемент $\star$, принимающий значение 1. При $k \geqslant 3$ также положим

$$Q = \{j \in B :\ j = (\underbrace{0,\dots,0}_{t_3}, 0, 1, \underbrace{0,\dots,0}_{k}, \underbrace{0,\dots,0}_{t_2}, 0, 1, \underbrace{0,\dots,0}_{k}, \underbrace{0,\dots,0}_{t_1}, 0, 1, \underbrace{0,\dots,0}_{k})\},$$

где $0 \leqslant t_1, t_2, t_3 \leqslant k-3$ и $t_1 + t_2 + t_3 = k-3$. Для $k = 2$ полагаем $D' = O' = Q = \varnothing$.

Лемма 13. *Для любого $j \in B$ имеет место один из следующих случаев*:

(1) $\ell'_j = 3$ *тогда и только тогда, когда* $j \in Q$, *если* НОД$(3, k) = 1$ ($\ell'_j = 3$ *тогда и только тогда, когда* $j \in Q$ *и* $(t_1, t_2, t_3) \neq (k'+1, k'+1, k'+1)$, *если* $k = 3k'$);
(2) $\ell'_j = 2$ *тогда и только тогда, когда* $j \in D \cup O$ *и* $j \notin Q$;
(3) *В остальных случаях* $\ell'_j = 1$.

Доказательство. Для $k = 2$ результат (1) очевиден, поскольку в этом случае $Q = \varnothing$. Итак, считаем, что $k \geqslant 3$. Если НОД$(3, k) = 1$, то $\ell_j = m$ по лемме 10. Тогда $\ell'_j \leqslant 3$. Во-первых, если $\ell'_j = 3$, то пусть $C'_j = \{j, j_1, j_2\}$, где $j \to$ $\to j_1 \to j_2 \to j$. При этом пусть для переходов $j \to j_1$, $j_1 \to j_2$ и $j_3 \to j$ требуются сдвиги кратностей по крайней мере $t_1 + k + 2$, $t_2 + k + 2$ и $t_3 + k + 2$ соответственно. Тогда $t_1 + k + 2 + t_2 + k + 2 + t_3 + k + 2 = m = 4k + 3$. Отсюда $t_1 + t_2 + t_3 = k - 3$.

При (t_1+k+2)-кратном сдвиге последовательности

$$j=(\underbrace{\star,\dots,\star}_{2k+1},\underbrace{0,\dots,0}_{k},0,1,\underbrace{0,\dots,0}_{k})$$

получаем

$$j_1=(\underbrace{0,\dots,0}_{t_1},0,1,\underbrace{0,\dots,0}_{k},\underbrace{\star,\dots,\star}_{2k+1},\underbrace{0,\dots,0}_{k-t_1}).$$

Так как $j_1\in B$, то

$$j_1=(\underbrace{0,\dots,0}_{t_1},0,1,\underbrace{0,\dots,0}_{k},\underbrace{\star,\dots,\star}_{k-t_1-1},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{t_1},\underbrace{0,\dots,0}_{k-t_1}).$$

При (t_2+k+2)-кратном сдвиге j_1 получаем

$$j_2=(\underbrace{0,\dots,0}_{t_2},0,1,\underbrace{0,\dots,0}_{t_1},\underbrace{0,\dots,0}_{k-t_1},\underbrace{0,\dots,0}_{t_1},0,1,\underbrace{0,\dots,0}_{k},\underbrace{\star,\dots,\star}_{k-t_1-1},\underbrace{0,\dots,0}_{k-t_2}).$$

Так как $j_2\in B$, то

$$j_2=(\underbrace{0,\dots,0}_{t_2},0,1,\underbrace{0,\dots,0}_{t_1},\underbrace{0,\dots,0}_{k-t_1},\underbrace{0,\dots,0}_{t_1},0,1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{k-t_1-t_2-2},1,\underbrace{0,\dots,0}_{t_2},\underbrace{0,\dots,0}_{k-t_2}).$$

Таким образом,

$$j=(\underbrace{0,\dots,0}_{k-t_1-t_2-2},1,\underbrace{0,\dots,0}_{k+1},\underbrace{0,\dots,0}_{t_2},1,\underbrace{0,\dots,0}_{k+1},\underbrace{0,\dots,0}_{t_1},1,\underbrace{0,\dots,0}_{k}),$$

и поэтому

$$j=(\underbrace{0,\dots,0}_{t_3},0,1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{t_2},0,1,\underbrace{0,\dots,0}_{k},\underbrace{0,\dots,0}_{t_1},0,1,\underbrace{0,\dots,0}_{k})\in Q.$$

В обратную сторону, если $j\in Q$, результат (1) очевиден. Во-вторых, с помощью аналогичных рассуждений получаем, что при $\ell'_j\geqslant 2$ последовательность j должна принадлежать D или O. Для любого $j\in D\cup O$ легко проверить, что $\ell'_j\geqslant 2$. Тогда из утверждения (1) с учетом $\ell'_j\leqslant 3$ получаем (2). Наконец, утверждение (3) очевидно. Для $k=3k'$ нетрудно убедиться, что $\ell'_j=1$, если $(t_1,t_2,t_3)=(k'+1,k'+1,k'+1)$. Из леммы 10 известно, что $\ell_j=\dfrac{m}{3}$ тогда и только тогда, когда $j=q^{k'}+q^{5k'+1}+q^{9k'+2}$, т.е. $j\in Q$ и $(t_1,t_2,t_3)=(k'+1,k'+1,k'+1)$. Итак, для $k=3k'$ результат также справедлив. ▲

Лемма 14. *В тех же обозначениях справедливы следующие утверждения*:
(1) $D'=O'=Q$;
(2) $D\cap O=Q$;
(3) $D\setminus Q\cup O\setminus Q=\bigcup\limits_{i\in D\setminus Q}C'_i=\bigcup\limits_{i\in O\setminus Q}C'_i$.

Доказательство. (1) Для любого элемента $j\in D'$ должно существовать некоторое целое число $0\leqslant t_1\leqslant k-3$, такое что

$$j=(0,\underbrace{\star,\dots,\star}_{k-t_1-2},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{t_1},\underbrace{0,\dots,0}_{k+1},1,\underbrace{0,\dots,0}_{k}),$$

где подпоследовательность $\underbrace{\star,\ldots,\star}_{k-t_1-2}$ содержит один и только один элемент $\star$, принимающий значение 1. Без ограничения общности будем считать, что

$$\underbrace{\star,\ldots,\star}_{k-t_1-2}=\underbrace{0,\ldots,0}_{a},1,\underbrace{0,\ldots,0}_{b}.$$

Тогда

$$j=(0,\underbrace{0,\ldots,0}_{a},1,0,\underbrace{0,\ldots,0}_{b},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{t_1},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{k}),$$

т.е. имеем

$$j=(0,\underbrace{0,\ldots,0}_{a},1,0,\underbrace{0,\ldots,0}_{k+1},\underbrace{0,\ldots,0}_{b},1,\underbrace{0,\ldots,0}_{t_1},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{k}).$$

Очевидно, что j принадлежит O', причем $t=2k-a-1$ и

$$\underbrace{\star,\ldots,\star}_{t-k-1}=\underbrace{0,\ldots,0}_{b},1,\underbrace{0,\ldots,0}_{a}.$$

Отсюда следует $D'\subset O'$. Аналогичными рассуждениями доказывается $O'\subset D'$. Таким образом, $D'=O'$. Утверждение $Q=D'$ очевидно.

(2) Из (1) получаем $Q\subset D\cap O$. Для любого $j\in D\cap O$ имеем

$$j=(\underbrace{\star,\ldots,\star}_{k-t_1-1},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{t_1},\underbrace{0,\ldots,0}_{k},0,1,\underbrace{0,\ldots,0}_{k})$$

для некоторого t, где $0\leqslant t_1\leqslant k-1$, поскольку $j\in D$. Так как

$$j\in O=\{j\in B:\ j=(\underbrace{0,\ldots,0}_{2k-t},1,\underbrace{0,\ldots,0}_{k},\underbrace{\star,\ldots,\star}_{t-k},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{k})\},$$

то

$$j=(\underbrace{0,\ldots,0}_{2k-t},1,\underbrace{0,\ldots,0}_{k},\underbrace{0,\ldots,0}_{t-k-t_1-1},1,\underbrace{0,\ldots,0}_{t_1},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{k})\in Q.$$

Таким образом, $D\cap O=Q$.

(3) Для любого $j\in D\setminus Q$ пусть $C'_j=\{j,j_1\}$. Ясно, что должно существовать некоторое $0\leqslant t_1\leqslant k-1$, такое что

$$j=(\underbrace{\star,\ldots,\star}_{k-t_1-1},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{k},\underbrace{0,\ldots,0}_{t_1},0,1,\underbrace{0,\ldots,0}_{k})$$

и

$$j_1=(\underbrace{0,\ldots,0}_{t_1},0,1,\underbrace{0,\ldots,0}_{k},\underbrace{\star,\ldots,\star}_{k-t_1-1},\underbrace{0,\ldots,0}_{k+1},1,\underbrace{0,\ldots,0}_{k}).$$

Это показывает, что $j\in O$, причем $t=2k-t_1-1$. Так как $\ell'_j=\ell'_{j_1}=2$, то $j\in O\setminus Q$. Для любого $i\in O\setminus Q$ пусть $C'_i=\{i,i_1\}$. Аналогичными рассуждениями можно показать, что $i_1\in D\setminus Q$. Поэтому $D\setminus Q\cup O\setminus Q=\bigcup\limits_{i\in D\setminus Q}C'_i=\bigcup\limits_{i\in O\setminus Q}C'_i$. ▲

При $k \geqslant 3$, если $(t_1, t_2, t_3) = (a, b, c)$ – некоторое решение уравнения $t_1 + t_2 + t_3 = k - 3$, то циклические сдвиги (c, a, b) и (b, c, a) также являются решениями этого уравнения. Обозначим эти три решения через $Q_{(a,b,c)}$. Тогда все решения уравнения $t_1 + t_2 + t_3 = k - 3$ можно представить в виде $\bigcup\limits_{i=0}^{e} Q_{(a_i,b_i,c_i)}$, где $\bigcap\limits_{i=0}^{e} Q_{(a_i,b_i,c_i)} = \varnothing$. Далее, положим $R = \{(a_i, b_i, c_i), 0 \leqslant i \leqslant e\}$ и

$$\overline{Q} = \Big\{ j \in Q : \; j = (\underbrace{0, \ldots, 0}_{c_i}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{b_i}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{a_i}, 0, 1, \underbrace{0, \ldots, 0}_{k}), \; (a_i, b_i, c_i) \in R \Big\}.$$

Следует отметить, что $Q_{(a,b,c)} \neq Q_{(a,c,b)}$, если числа a, b, c попарно различны, и $Q_{(a,b,c)} = Q_{(a,c,b)}$, если среди них есть два одинаковых.

Лемма 15. *Для любых трех различных элементов $j, j_1, j_2 \in B$ неравенство $C_j \cap C_{j_1} \cap C_{j_2} \neq \varnothing$ выполнено тогда и только тогда, когда существует некоторое $J \in \overline{Q}$, такое что $C'_J = \{j, j_1, j_2\}$.*

Доказательство. Если $C_j \cap C_{j_1} \cap C_{j_2} \neq \varnothing$, то $C_j = C_{j_1} = C_{j_2}$. Таким образом, $j_1, j_2 \in C'_j$. Из утверждения (1) леммы 13 получаем $j, j_1, j_2 \in Q$. Без ограничения общности будем считать, что $j \to j_1 \to j_2$ в C'_j. Кроме того, пусть

$$j = (\underbrace{0, \ldots, 0}_{c}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{b}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{a}, 0, 1, \underbrace{0, \ldots, 0}_{k}) \in Q.$$

Тогда

$$j_1 = (\underbrace{0, \ldots, 0}_{a}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{c}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{b}, 0, 1, \underbrace{0, \ldots, 0}_{k}) \in Q$$

и

$$j_2 = (\underbrace{0, \ldots, 0}_{b}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{a}, 0, 1, \underbrace{0, \ldots, 0}_{k}, \underbrace{0, \ldots, 0}_{c}, 0, 1, \underbrace{0, \ldots, 0}_{k}) \in Q.$$

Отсюда следует, что один из элементов j, j_1 и j_2 принадлежит $\overline{Q}$, обозначим его через J. В обратную сторону утверждение тривиально. ▲

Для удобства обозначим

$\mathcal{A} = \{i : \; i \in \overline{A}$ и $i \notin \overline{B}_1 \cup \overline{B}_2\}$,
$\mathcal{B} = \{j : \; j \in B$ и $j \notin D \cup O \cup B_1 \cup B_2\}$,
$\mathcal{B}_1 = \{j : \; j \in \overline{B}_1 \cup \overline{B}_2$ и $j \notin \overline{B}'_1\}$

соответственно.

Лемма 16. *В тех же обозначениях справедливы следующие утверждения*:

(1) $|\mathcal{A}| = 2^{2k} + 2^k - 2^{k-1} + k - 2$;
(2) $|\mathcal{B}| = 2^{2k+1} - 2^{k+1} - 2^k - 2^{k-1} + k + 1$;
(3) $|\mathcal{B}_1| = 2^k + 2^{k-1} - 2k + 2$;
(4) $|D \setminus Q| = 2^k - \dfrac{(k-1)(k-2)}{2} - 1$;
(5) $|\overline{Q}| = \begin{cases} \dfrac{(k-1)(k-2)}{6}, & \text{НОД}(3, k) = 1, \\ \dfrac{(k-1)(k-2)-2}{6} + 1, & k = 3k'. \end{cases}$

Доказательство. Результат следует из определений соответствующих множеств. ▲

Теорема 3. *Пусть s^∞ – последовательность типа* (3) *с мономом*

$$f(x) = x^{q^{(3m-1)/4}+(q^{(m-1)/2}-1)/(q-1)}$$

над полем $\mathbb{F}_{q^m}$. Тогда справедливы следующие утверждения.

(1) *Если $k = 0$ или 1, то линейная сложность L_s и минимальный многочлен $M_s(x)$ для s^∞ имеют вид*

$$L_s = \begin{cases} 3(N_p(2)+1) + N_P(3), & k = 0, \\ 7(3N_p(2) + N_p(4) + 5) + N_p(7), & k = 1, \end{cases}$$

и

$$M_s(x) = \begin{cases} (x-1)^{N_p(3)} m_{\alpha^{-1}}(x)^{N_p(2)} m_{\alpha^{-(q^2+1)}}(x), & k = 0, \\ (x-1)^{N_p(7)} m_{\alpha^{-1}}(x)^{N_p(4)} \prod\limits_{i\in D_1} m_{\alpha^{-i}}(x) \prod\limits_{i\in D_2} m_{\alpha^{-i}}(x)^{N_p(2)}, & k = 1, \end{cases}$$

где

$$D_1 = \{1+q+q^2, 1+q+q^5, 1+q^2+q^5, q+q^2+q^5, 1+q+q^2+q^5\},$$
$$D_2 = \{1+q, 1+q^2, q+q^5\}.$$

(2) *Если $k \geqslant 2$ и* НОД$(3,k) = 1$, *то линейная сложность L_s и минимальный многочлен $M_s(x)$ для s^∞ имеют вид*

$$L_s = \Bigg\{ \sum_{s\in\mathcal{A}\setminus\{0\}} N_p(m^s - 2k - 1) + \sum_{s\in\mathcal{B}_1} N_p(m^s - 2k) + \sum_{s\in\overline{B}'_1} N_p(m^s - 2k + 1) + \\ + \sum_{s\in\mathcal{B}} 1 + \sum_{s\in D\setminus Q} N_p(2) + \sum_{s\in\overline{Q}} N_p(3) \Bigg\} m + N_p(m)$$

и

$$M_s(x) = (x-1)^{N_p(m)} \prod_{s\in\mathcal{A}\setminus\{0\}} m_{\alpha^{-s}}(x)^{N_p(m^s-2k-1)} \prod_{s\in\mathcal{B}_1} m_{\alpha^{-s}}(x)^{N_p(m^s-2k)} \times \\ \times \prod_{s\in\overline{B}'_1} m_{\alpha^{-s}}(x)^{N_p(m^s-2k+1)} \prod_{s\in\mathcal{B}} m_{\alpha^{-s}}(x) \prod_{s\in D\setminus Q} m_{\alpha^{-s}}(x)^{N_p(2)} \prod_{s\in\overline{Q}} m_{\alpha^{-s}}(x)^{N_p(3)}.$$

(3) *Если $k = 3k'$, то линейная сложность L_s и минимальный многочлен $M_s(x)$ для s^∞ имеют вид*

$$L_s = \Bigg\{ \sum_{s\in\mathcal{A}\setminus\{0\}} N_p(m^s - 2k - 1) + \sum_{s\in\mathcal{B}_1} N_p(m^s - 2k) + \sum_{s\in\overline{B}'_1} N_p(m^s - 2k + 1) + \\ + \sum_{s\in\mathcal{B}^*} 1 + \sum_{s\in D\setminus Q} N_p(2) + \sum_{s\in\overline{Q}^*} N_p(3) \Bigg\} m + \frac{m}{3} + N_p(m)$$

и

$$M_s(x) = m_{\alpha^{-s_0}}(x)^{N_p(3)}(x-1)^{N_p(m)} \prod_{s\in\mathcal{A}\setminus\{0\}} m_{\alpha^{-s}}(x)^{N_p(m^s-2k-1)} \times$$
$$\times \prod_{s\in\mathcal{B}_1} m_{\alpha^{-s}}(x)^{N_p(m^s-2k)} \prod_{s\in\overline{B}'_1} m_{\alpha^{-s}}(x)^{N_p(m^s-2k+1)} \prod_{s\in\mathcal{B}^*} m_{\alpha^{-s}}(x) \times$$
$$\times \prod_{s\in D\setminus Q} m_{\alpha^{-s}}(x)^{N_p(2)} \prod_{s\in\overline{Q}^*} m_{\alpha^{-s}}(x)^{N_p(3)},$$

где $\mathcal{B}^* = \mathcal{B}\setminus\{s_0 = q^{k'} + q^{5k'+1} + q^{9k'+2}\}$.

Доказательство. (1) При $k=0$ имеем

$$s_t = \mathrm{Tr}(f(\alpha^t+1)) = \mathrm{Tr}\big((\alpha^t+1)^{q^2+1}\big) = \mathrm{Tr}\big(1+\alpha^t+(\alpha^t)^{q^2}+(\alpha^t)^{1+q^2}\big) =$$
$$= \mathrm{Tr}(1) + 2\,\mathrm{Tr}(\alpha^t) + \mathrm{Tr}\big((\alpha^t)^{1+q^2}\big).$$

Аналогично, при $k=1$ имеем

$$s_t = \mathrm{Tr}(f(\alpha^t+1)) = \mathrm{Tr}\big((\alpha^t+1)^{q^5+q^2+q+1}\big) = \mathrm{Tr}(1) + 4\,\mathrm{Tr}(\alpha^t) +$$
$$+ \sum_{s\in D_1} \mathrm{Tr}\big((\alpha^t)^s\big) + 2\sum_{s\in D_2} \mathrm{Tr}\big((\alpha^t)^s\big),$$

где $D_1 = \{1+q+q^2, 1+q+q^5, 1+q^2+q^5, q+q^2+q^5, 1+q+q^2+q^5\}$ и $D_2 = \{1+q, 1+q^2, q+q^5\}$. Поэтому требуемые результаты о линейной сложности L_s и минимальном многочлене $M_s(x)$ теперь вытекают из леммы 4.

(2) Если $k \geqslant 2$ и НОД$(3,k)=1$, то из предыдущих рассуждений с учетом формулы (3) получаем

$$s_t = \mathrm{Tr}(f(\alpha^t+1)) = \mathrm{Tr}\Big(\sum_{i\in A}(\alpha^t)^i + \sum_{i\in B}(\alpha^t)^i\Big) = \mathrm{Tr}\Big(\sum_{s\in\mathcal{A}}\sum_{i\in C'_s}(\alpha^t)^i +$$
$$+ \sum_{s\in\mathcal{B}_1}\sum_{i\in C'_s}(\alpha^t)^i + \sum_{s\in\overline{B}'_1}\sum_{i\in C'_s}(\alpha^t)^i + \sum_{i\in\mathcal{B}}(\alpha^t)^i + \sum_{s\in D\setminus Q}\sum_{i\in C'_s}(\alpha^t)^i +$$
$$+ \sum_{s\in\overline{Q}}\sum_{i\in C'_s}(\alpha^t)^i\Big) = \mathrm{Tr}(1) + \sum_{s\in\mathcal{A}\setminus\{0\}}(m^s-2k-1)\,\mathrm{Tr}\big((\alpha^t)^s\big) +$$
$$+ \sum_{s\in\mathcal{B}_1}(m^s-2k)\,\mathrm{Tr}\big((\alpha^t)^s\big) + \sum_{s\in\overline{B}'_1}(m^s-2k+1)\,\mathrm{Tr}\big((\alpha^t)^s\big) + \sum_{s\in\mathcal{B}}\mathrm{Tr}\big((\alpha^t)^s\big) +$$
$$+ 2\sum_{s\in D\setminus Q}\mathrm{Tr}\big((\alpha^t)^s\big) + 3\sum_{s\in\overline{Q}}\mathrm{Tr}\big((\alpha^t)^s\big).$$

Поэтому требуемые результаты о линейной сложности L_s и минимальном многочлене $M_s(x)$ теперь вытекают из леммы 4.

(3) Результат следует из леммы 10 с учетом доказательства утверждения (2). ▲

Теорема 4. *Пусть C_s – циклический код, определяемый последовательностью s^∞ из теоремы* 3. *Тогда C_s имеет параметры $[n, n-L_s, d]$ и порождающий многочлен $M_s(x)$, где L_s и $M_s(x)$ указаны в теореме* 3.

Для любого $N_p(*)$ из теоремы 3 положим $N_P(*)=1$. Тогда имеет место

Следствие 3. *При $k \geqslant 2$ положим $\mathcal{R} = \mathcal{A} \cup \mathcal{B}_1 \cup \overline{B}_1' \cup \mathcal{B} \cup (D \setminus Q) \cup \overline{Q}$ и $N_P(*) = 1$ для любого $N_p(*)$ из теоремы 3. Тогда код C_s, определяемый последовательностью s^∞, имеет параметры $[n, n - L_s, d]$ и порождающий многочлен $M_s(x)$, где*

$$L_s = \begin{cases} m\Big(3 \cdot 2^{2k} - 2^{k-1} - \dfrac{(k-1)(k-2)}{3} + k - 2\Big) + 1, & \text{НОД}(3,k) = 1, \\ m\Big(3 \cdot 2^{2k} - 2^{k-1} - \dfrac{(k-1)(k-2)+1}{3} + k - 2\Big) + \dfrac{m}{3} + 1, & k = 3k', \end{cases}$$

и

$$M_s(x) = \prod_{s \in \mathcal{R}} m_{\alpha^{-s}}(x).$$

Доказательство. Результат следует из теоремы 3 и леммы 16. ▲

Для $q = 2$ хорошо известно [27, 28], что моном $f(x) = x^{2^{(m-1)/2}+2^{(3m-1)/4}-1}$ является почти совершенно нелинейной функцией над $\mathbb{F}_{2^m}$, где $m \equiv 3 \pmod 4$. Теперь рассмотрим двоичные циклические коды, определяемые мономами такого типа. Из теоремы 3 получаем

Следствие 4. *Пусть $q = 2$. Тогда s^∞ – двоичная последовательность с*

$$f(x) = x^{2^{(m-1)/2}+2^{(3m-1)/4}-1}$$

над $\mathbb{F}_{2^m}$. Кроме того, справедливы следующие три утверждения:

(1) *Если $k = 0$ или 1, то линейная сложность L_s и минимальный многочлен $M_s(x)$ для s^∞ имеют вид*

$$L_s = \begin{cases} 4, & k = 0, \\ 36, & k = 1, \end{cases}$$

и

$$M_s(x) = \begin{cases} (x-1) m_{\alpha^{-(2^2+1)}}(x), & k = 0, \\ (x-1) \prod\limits_{i \in D_1} m_{\alpha^{-i}}(x), & k = 1, \end{cases}$$

где $D_1 = \{7, 35, 37, 38, 39\}$.

(2) *Если $k \geqslant 2$ и $\text{НОД}(3,k) = 1$, то линейная сложность L_s и минимальный многочлен $M_s(x)$ для s^∞ имеют вид*

$$L_s = \Bigg\{ \sum_{s \in \mathcal{A} \setminus \{0\}} N_2(m^s - 2k - 1) + \sum_{s \in \mathcal{B}_1} N_2(m^s - 2k) + \sum_{s \in \overline{B}_1'} N_2(m^s - 2k + 1) + \\ + \sum_{s \in \mathcal{B} \cup \overline{Q}} 1 \Bigg\} m + 1$$

и

$$M_s(x) = (x-1) \prod_{s \in \mathcal{A} \setminus \{0\}} m_{\alpha^{-s}}(x)^{N_2(m^s - 2k - 1)} \prod_{s \in \mathcal{B}_1} m_{\alpha^{-s}}(x)^{N_2(m^s - 2k)} \times \\ \times \prod_{s \in \overline{B}_1'} m_{\alpha^{-s}}(x)^{N_2(m^s - 2k + 1)} \prod_{s \in \mathcal{B} \cup \overline{Q}} m_{\alpha^{-s}}(x).$$

(3) *Если* $k = 3k'$, *то линейная сложность* L_s *и минимальный многочлен* $M_s(x)$ *для* s^∞ *имеют вид*

$$L_s = \Bigg\{ \sum_{s\in\mathcal{A}\setminus\{0\}} N_2(m^s - 2k - 1) + \sum_{s\in\mathcal{B}_1} N_2(m^s - 2k) + \sum_{s\in\overline{B}'_1} N_2(m^s - 2k + 1) +$$

$$+ \sum_{s\in\mathcal{B}^*\cup\overline{Q}^*} 1 \Bigg\} m + \frac{m}{3} + 1$$

и

$$M_s(x) = (x-1) m_{\alpha^{-s_0}}(x) \prod_{s\in\mathcal{A}\setminus\{0\}} m_{\alpha^{-s}}(x)^{N_2(m^s-2k-1)} \prod_{s\in\mathcal{B}_1} m_{\alpha^{-s}}(x)^{N_2(m^s-2k)} \times$$

$$\times \prod_{s\in\overline{B}'_1} m_{\alpha^{-s}}(x)^{N_2(m^s-2k+1)} \prod_{s\in\mathcal{B}^*\cup\overline{Q}^*} m_{\alpha^{-s}}(x),$$

где $\mathcal{B}^* = \mathcal{B} \setminus \{s_0 = 2^{k'} + 2^{5k'+1} + 2^{9k'+2}\}$.

Таким образом, для двоичного циклического кода C_s, определяемого мономом $f(x) = x^{2^{(m-1)/2}+2^{(3m-1)/4}-1}$, справедлива

Теорема 5. *Двоичный циклический код* C_s, *определяемый последовательностью* s^∞ *из следствия* 4, *имеет параметры* $[n, n - L_s, d]$ *и порождающий многочлен* $M_s(x)$, *указанные в следствии* 4. *Кроме того, для минимального расстояния* d *имеет место следующая граница*:

$$d \geqslant 2^{k+1} + 2.$$

Доказательство. Утверждение о порождающем многочлене и размерности кода C_s вытекают из определения кода и следствия 4. Остается доказать справедливость нижней границы на минимальное расстояние d. Нетрудно вычислить, что $d \geqslant 4$ при $k = 0$ и $d \geqslant 6$ при $k = 1$. Далее, согласно определению множества $\mathcal{B}$ нетрудно увидеть, что $\{j + 2^{k+1} + 2^{2k} + 2^{3k+2} : j = 0, 1, 2, \ldots, 2^{k+1} - 1\} \subseteq \mathcal{B}^*$. Отсюда следует, что α^i является корнем многочлена, взаимного к $M_s(x)$, для любого $i \in \{j+2^{k+1}+2^{2k}+2^{3k+2} : j = 0, 1, 2, \ldots, 2^{k+1}-1\}$. Заметим, что коды, порожденные многочленом $M_s(x)$ и его взаимным многочленам, имеют одинаковое распределение весов. Согласно границе БЧХ $d \geqslant 2^{k+1} + 1$. Очевидно, что циклический код C_s является кодом с четным весами. Следовательно, $d \geqslant 2^{k+1} + 2$. При $k = 0$ и 1 минимальное расстояние d удовлетворяет неравенству $d \geqslant 2^{k+1} + 2$, что и завершает доказательство. ▲

Замечание 3. Результаты этого пункта для $q = 2$ дают некоторые ответы на открытую проблему 3, поставленную в работе [1]. Размерность и порождающий многочлен этого подкласса двоичных циклических кодов имеют широкий диапазон значений. Кроме того, получена нижняя граница на расстояние для этого подкласса циклических кодов.

Пример 7. Пусть $(q, k, m) = (2, 1, 7)$, и пусть α – примитивный элемент поля $\mathbb{F}_{2^7}$, такой что $\alpha^7 + \alpha + 1 = 0$. Тогда порождающий многочлен кода C_s имеет вид

$$M_s(x) = x^{36} + x^{35} + x^{32} + x^{30} + x^{29} + x^{28} + x^{27} + x^{22} + x^{21} + x^{19} + x^{17} +$$
$$+ x^{16} + x^{15} + x^{14} + x^{12} + x^{11} + x^6 + x^2 + x + 1,$$

а C_s является двоичным циклическим $[127, 91, 10]$-кодом. Его двойственный код – двоичный циклический $[127, 36, 32]$-код.

§ 4. Заключение

Построены три класса циклических кодов на основе некоторых последовательностей с мономами специальных типов. Размерности и порождающие многочлены этих классов q-ичных циклических кодов имеют широкий диапазон значений. Кроме того, рассмотрено минимальное расстояние таких циклических кодов. Следует отметить, что многие из представленных кодов оптимальны или почти оптимальны согласно таблицам [2].

СПИСОК ЛИТЕРАТУРЫ

1. *Ding C., Zhou Z.* Binary Cyclic Codes from Explicit Polynomials over GF(2^m) // Discrete Math. 2014. V. 321. P. 76–89.
2. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available at `http://www.codetables.de`.
3. *Chien R.T.* Cyclic Decoding Procedures for Bose–Chaudhuri–Hocquenghem Codes // IEEE Trans. Inform. Theory. 1964. V. 10. № 4. P. 357–363.
4. *Forney G.D., Jr.* On Decoding BCH Codes // IEEE Trans. Inform. Theory. 1965. V. 11. № 4. P. 549–557.
5. *Prange E.* Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms. Tech. Rep. TN-58-156. Air Force Cambridge Research Center. Bedford, MA, USA. April, 1958.
6. *Berlekamp E.R., Justesen J.* Some Long Cyclic Linear Binary Codes Are Not So Bad // IEEE Trans. Inform. Theory. 1974. V. 20. № 3. P. 351–356.
7. *Calderbank A.R., Li W.-C.W., Poonen B.* A 2-adic Approach to the Analysis of Cyclic Codes // IEEE Trans. Inform. Theory. 1997. V. 43. № 3. P. 977–986.
8. *Kai X., Zhu S.* On Cyclic Self-Dual Codes // Appl. Algebra Engrg. Comm. Comput. 2008. V. 19. № 6. P. 509–525.
9. *Li C., Li N., Helleseth T., Ding C.* The Weight Distributions of Several Classes of Cyclic Codes from APN Monomials // IEEE Trans. Inform. Theory. 2014. V. 60. № 8. P. 4710–4721.
10. *Liu L., Xie X., Li L., Zhu S.* The Weight Distributions of Two Classes of Nonbinary Cyclic Codes with Few Weights // IEEE Commun. Lett. 2017. V. 21. № 11. P. 2336–2339.
11. *Luo J., Feng K.* Cyclic Codes and Sequences from Generalized Coulter–Matthews Function // IEEE Trans. Inform. Theory. 2008. V. 54. № 12. P. 5345–5353.
12. *Martinez-Pérez C., Willems W.* Is the Class of Cyclic Codes Asymptotically Good? // IEEE Trans. Inform. Theory. 2006. V. 52. № 2. P. 696–700.
13. *Moreno O., Kumar P.V.* Minimum Distance Bounds for Cyclic Codes and Deligne's Theorem // IEEE Trans. Inform. Theory. 1993. V. 39. № 5. P. 1524–1534.
14. *Rao A., Pinnawala N.* A Family of Two-Weight Irreducible Cyclic Codes // IEEE Trans. Inform. Theory. 2010. V. 56. № 6. P. 2568–2570.
15. *Roth R.M., Seroussi G.* On Cyclic MDS Codes of Length q over GF(q) // IEEE Trans. Inform. Theory. 1986. V. 32. № 2. P. 284–285.
16. *van Lint J.H., Wilson R.M.* On the Minimum Distance of Cyclic Codes // IEEE Trans. Inform. Theory. 1986. V. 32. № 1. P. 23–40.
17. *Zeng X., Hu L., Jiang W., Yue Q., Cao X.* The Weight Distribution of a Class of p-ary Cyclic Codes // Finite Fields Appl. 2010. V. 16. № 1. P. 56–73.
18. *Ding C.* Cyclic Codes from Some Monomials and Trinomials // SIAM J. Discrete Math. 2013. V. 27. № 4. P. 1977–1994.
19. *Ding C.* A Sequence Construction of Cyclic Codes over Finite Fields // Cryptogr. Commun. 2018. V. 10. № 2. P. 319–341.
20. *Rajabi Z., Khashyarmanesh K.* Some Cyclic Codes from Some Monomials // Appl. Algebra Engrg. Comm. Comput. 2017. V. 28. № 6. P. 469–495.
21. *Tang C., Qi Y., Xu M.* A Note on Cyclic Codes from APN Functions // Appl. Algebra Engrg. Comm. Comput. 2014. V. 25. № 1–2. P. 21–37.
22. *Ding C., Helleseth T.* Optimal Ternary Cyclic Codes from Monomials // IEEE Trans. Inform. Theory. 2013. V. 59. № 9. P. 5898–5904.

23. *Huffman W.C., Pless V.* Fundamentals of Error-Correcting Codes. Cambridge: Cambridge Univ. Press, 2003.
24. *Ding C., Xiao G., Shan W.* The Stability Theory of Stream Ciphers. Lect. Notes Comp. Sci. V. 561. Heidelberg: Springer, 1991.
25. *El Rouayheb S.Y., Georghiades C.N., Soljanin E., Sprintson A.* Bounds on Codes Based on Graph Theory // Proc. 2007 IEEE Int. Sympos. on Information Theory (ISIT'2007). Nice, France. June 24–29, 2007. P. 1876–1879.
26. *Lucas E.* Théorie des fonctions numériques simplement périodiques // Amer. J. Math. 1878. V. 1. № 4. P. 289–321.
27. *Dobbertin H.* Almost Perfect Nonlinear Power Functions on GF(2^n): The Niho Case // Inform. and Comput. 1999. V. 151. № 1–2. P. 57–72.
28. *Hollmann H.D.L., Xiang Q.* A Proof of the Welch and Niho Conjectures on Cross-Correlations of Binary m-Sequences // Finite Fields Appl. 2001. V. 7. № 2. P. 253–286.

Ли Ланьцян
Чжу Шисинь
Лю Ли
Кай Сяошань
Школа математики, Технологический университет Хэфэй, провинция Аньхой, КНР
lilanqiang716@126.com
zhushixinmath@hfut.edu.cn
liuli-1128@163.com
kxs6@sina.com

Поступила в редакцию
30.09.2018
После доработки
29.04.2019
Принята к публикации
10.06.2019