Скрученные линейные рекурренты максимального периода над кольцами Галуа*

М. А. ГОЛЬТВАНИЦА, С. Н. ЗАЙЦЕВ
Центр сертификационных исследований

А. А. НЕЧАЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: alexnechaev@inbox.ru

УДК 519.7

Ключевые слова: скрученная линейная рекуррентная последовательность, кольцо Галуа, автоморфизм Фробениуса, линейная рекуррентная последовательность максимального периода, ранг.

Аннотация

Пусть p — простое число, $R = GR(q^d, p^d)$ — кольцо Галуа мощности $q^d = p^{rd}$ и характеристики p^d, $S = GR(q^{nd}, p^d)$ — его расширение степени n, $\check{S}$ — кольцо всех линейных преобразований модуля ${}_RS$. Изучаются последовательности v над кольцом S с линейным законом рекурсии порядка m, коэффициенты которого выбираются из кольца $\check{S}$, т. е. линейные рекуррентные последовательности порядка m над модулем ${}_{\check{S}}S$ (скрученные ЛРП). Доказано, что максимум периодов таких последовательностей есть $\tau = (q^{nm} - 1)p^{d-1}$. Найдена общая характеризация множества всех скрученных ЛРП порядка m и периода τ, указан простой метод построения значительного класса таких последовательностей (линеаризуемых скрученных ЛРП максимального периода) и доказано, что их ранги как линейных рекуррент над модулями ${}_SS$ и ${}_RS$ могут совпадать и равняться mn. Найдено число линеаризуемых скрученных ЛРП ранга m и периода τ.

Abstract

M. A. Goltvanitsa, S. N. Zaitsev, A. A. Nechaev, Skew linear recurring sequences of maximal period over Galois rings, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 3, pp. 5—23.

Let p be a prime number, $R = GR(q^d, p^d)$ be a Galois ring of $q^d = p^{rd}$ elements and of characteristic p^d. Denote by $S = GR(q^{nd}, p^d)$ a Galois extension of the ring R of dimension n and by $\check{S}$ the ring of all linear transformations of the module ${}_RS$. We call a sequence v over the ring S with the law of recursion

$$\text{for all } i \in \mathbb{N}_0\colon\ v(i+m) = \psi_{m-1}\big(v(i+m-1)\big) + \cdots + \psi_0\big(v(i)\big), \quad \psi_0, \ldots, \psi_{m-1} \in \check{S}$$

(i.e., a linear recurring sequence of order m over the module ${}_{\check{S}}S$) a skew LRS over S. It is known that the period $T(v)$ of such a sequence satisfies the inequality $T(v) \leqslant \tau = (q^{nm} - 1)p^{d-1}$. If $T(v) = \tau$, then we call v a skew LRS of maximal period (a skew MP LRS) over S. A new general characterization of skew MP LRS in terms of

*Работа поддержана грантом Президента РФ НШ-8.2010.10.

Фундаментальная и прикладная математика, 2011/2012, том 17, № 3, с. 5—23.

coordinate sequences corresponding to some basis of a free module ${}_RS$ is given. A simple constructive method of building a big enough class of skew MP LRS is stated, and it is proved that the linear complexity of some of them (the rank of the linear recurring sequence) over the module ${}_SS$ is equal to mn, i.e., to the linear complexity over the module ${}_RS$.

1. Введение. Основные результаты

Всюду далее $R = GR(q^d, p^d)$ — кольцо Галуа, $S = GR(q^{nd}, p^d)$ — расширение Галуа степени n кольца R [3, 9, 13].

Известно, что группа $\mathrm{Aut}(S/R)$ автоморфизмов кольца S над R является циклической порядка n. Пусть σ — её порождающий элемент и $\check{S} = S^{\sigma}\langle\sigma\rangle$ — скрученное групповое кольцо группы $\langle\sigma\rangle$ над кольцом S, т. е. совокупность формальных сумм

$$\psi = \sum_{i=0}^{n-1} s_i\sigma^i, \quad s_0, \ldots, s_{n-1} \in S,$$

с естественным сложением и умножением, определяемым по дистрибутивности из тождества $\sigma s = \sigma(s)\sigma$ для любого $s \in S$.

Каждый элемент $\psi \in \check{S}$ задаёт эндоморфизм модуля ${}_RS$, действие которого на элементе $s \in S$ определяется равенством

$$\psi(s) = \sum_{i=0}^{n-1} s_i\sigma^i(s),$$

и этим задаётся изоморфизм

$$\check{S} \cong \mathrm{End}({}_RS) \cong R_{n,n}, \tag{1.1}$$

где $R_{n,n}$ — кольцо всех $(n \times n)$-матриц над R. Таким образом на кольце S задаётся структура левого $\check{S}$-модуля.

Множество $S^{\langle 1\rangle}$ всех последовательностей над S является левым модулем над кольцом многочленов $\check{S}[x]$, в котором умножение многочлена

$$A(x) = \sum_{i\geqslant 0} a_i x^i \in \check{S}[x]$$

на последовательность $v \in S^{\langle 1\rangle}$ определяется равенством

$$A(x)v = w \in S^{\langle 1\rangle} \colon w(j) = \sum_{i\geqslant 0} a_i\big(v(i+j)\big) \quad \text{для} \quad j \geqslant 0.$$

Последовательность $v \in S^{\langle 1\rangle}$ назовём *скрученной линейной рекуррентной последовательностью* (ЛРП) порядка $m > 0$ над кольцом S, если она есть ЛРП порядка m над модулем ${}_{\check{S}}S$ [10], т. е.

$$\Psi(x)v = 0 \tag{1.2}$$

для некоторого унитарного многочлена

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \ldots - \psi_0 \in \check{S}[x] \tag{1.3}$$

степени m, называемого *характеристическим многочленом ЛРП* v, иначе говоря, если последовательность v удовлетворяет некоторому закону рекурсии

$$v(i+m) = \psi_{m-1}\big(v(i+m-1)\big) + \ldots + \psi_0\big(v(i)\big) \quad \text{для всех} \quad i \in \mathbb{N}_0. \tag{1.4}$$

Совокупность всех ЛРП v над кольцом S с характеристическим многочленом Ψ обозначим через $L_S(\Psi)$.

Заметим, в частности, что любая ЛРП u порядка m над S, т. е. последовательность, аннулируемая некоторым унитарным многочленом $G(x) \in S[x]$ степени m, является скрученной ЛРП порядка m над S. Известно [5, 6, 9], что её период удовлетворяет условиям

$$T(u) \leqslant T(G) \leqslant \tau = (q^{nm} - 1)p^{d-1}.$$

Здесь $T(G)$ — период многочлена $G(x) \in S[x]$. В случае когда

$$T(G) = \tau = (|\bar{S}|^m - 1)p^{d-1},$$

многочлен $G(x)$ называется *многочленом максимального периода над кольцом* S. Указанная верхняя оценка дословно обобщается на периоды скрученных ЛРП.

Предложение 1. *Для любой скрученной ЛРП v порядка m над S существует унитарный многочлен $F(x) \in R[x]$ степени mn, такой что*

$$v \in L_S(F). \tag{1.5}$$

При этом справедливы соотношения

$$T(v) \mid T(F), \quad T(F) \leqslant \tau = (q^{nm} - 1)p^{d-1}. \tag{1.6}$$

В случае когда $T(v) = \tau$, будем называть последовательность v скрученной ЛРП *максимального периода* (МП ЛРП).

Для проведения некоторых доказательств и сравнения наших результатов с результатами предшествующих авторов полезно сформулировать обсуждаемые понятия на матричном языке.

Зафиксируем базис $\vec{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ свободного модуля ${}_RS$ и обозначим через $a^{\downarrow} = (a_0, \ldots, a_{n-1})^{\mathrm{T}} \in R^{(n)}$ столбец координат элемента $a \in S$ в базисе $\vec{\alpha}$:

$$a = \sum_{i=0}^{n-1} a_i\alpha_i = \sum_{i=0}^{n-1} \alpha_i a_i = \vec{\alpha}a^{\downarrow}.$$

Тогда каждому линейному преобразованию $\psi \in \check{S}$ модуля ${}_RS$ соответствует единственная матрица $A(\psi) \in R_{n,n}$, такая что для любого $a \in S$

$$\psi(a)^{\downarrow} = A(\psi)a^{\downarrow},$$

называемая *матрицей линейного преобразования ψ в базисе $\vec{\alpha}$*.

Очевидно, последовательность $v \in S^{\langle 1\rangle}$ является скрученной ЛРП порядка m, т. е. удовлетворяет некоторому соотношению (1.4), тогда и только тогда, когда столбцы координат $v^{\downarrow}(i)$ членов этой последовательности в базисе $\vec{\alpha}$ удовлетворяют соотношению

$$v^{\downarrow}(i+m) = A(\psi_{m-1})v^{\downarrow}(i+m-1) + \ldots + A(\psi_0)v^{\downarrow}(i) \quad \text{для всех} \quad i \in \mathbb{N}_0. \quad (1.7)$$

Соотношение (1.8) будем называть *законом рекурсии скрученной ЛРП v в матричном виде*.

Согласно (1.1) матрицы $A_s = A(\psi_s) \in R_{n\times n}$, $s \in \overline{0, m-1}$, в (1.7) могут быть произвольными, и закон рекурсии (1.7) можно записать компактнее:

$$\text{для всех } i \in \mathbb{N}_0\colon\ v^{\downarrow}(i+m) = A_{m-1}v^{\downarrow}(i+m-1) + \ldots + A_0v^{\downarrow}(i), \quad A_0, \ldots, A_{m-1} \in R_{n,n}. \quad (1.8)$$

Именно такие последовательности изучались ранее в [7, 10, 14—17], но только в случае, когда R — поле.

При заданном базисе $\vec{\alpha}$ модуля ${}_RS$ для произвольной последовательности $v \in S^{\langle 1\rangle}$ существует единственный набор последовательностей $v_0, \ldots, v_{n-1} \in \in R^{\langle 1\rangle}$, такой что

$$v = v_0\alpha_0 + v_1\alpha_1 + \ldots + v_{n-1}\alpha_{n-1}. \quad (1.9)$$

Будем называть $v_0, \ldots, v_{n-1}$ *координатными последовательностями* последовательности v (в базисе $\vec{\alpha}$).

В данной работе изучаются скрученные МП ЛРП над кольцами Галуа. Приводится общая характеризация класса всех скрученных МП ЛРП, указывается метод построения значительного класса таких последовательностей и исследуются ранги скрученных МП ЛРП как линейных рекуррент над модулями ${}_RS$ и ${}_SS$. Также исследуются координатные последовательности рекуррент из этого класса. Полученные результаты частично являются новыми даже для случая, когда R — поле, и хорошо иллюстрируют эффективность изучения последовательностей вида (1.8) как рекуррентных последовательностей (1.4) над модулем ${}_{\tilde{S}}S$.

Всюду далее для $i, t \in \mathbb{N}_0$ используется обозначение

$$v[\overline{i, i+t}] = \big(v(i), v(i+1), \ldots, v(i+t)\big).$$

Предлагается следующая общая характеризация класса скрученных МП ЛРП.

Теорема 2. *Последовательность $v \in S^{\langle 1\rangle}$ является скрученной МП ЛРП порядка m тогда и только тогда, когда*

$$v[\overline{i, i+m-1}] \notin (pS)^m \quad \text{для всех} \quad i \in \mathbb{N}_0 \quad (1.10)$$

и существует многочлен максимального периода $F(x) \in R[x]$ степени mn, такой что выполняется условие (1.5).

Любая скрученная МП ЛРП v является реверсивной (*чисто периодической*), *и при выполнении условия* (1.5) *система координатных последовательностей*

$v_0, \dots, v_{n-1}$ из её разложения (1.9) *является линейно независимой системой МП ЛРП из* $L_R\big(F(x)\big)$.

Эта теорема существенно усиливает результат работы [15], в которой отмечено лишь, что если S — поле и R — его подполе, то координатные последовательности $v_0, \dots, v_{n-1}$ являются линейными рекуррентами максимального периода из $L_R\big(F(x)\big)$. При этом ничего не говорится о линейной независимости этой системы последовательностей.

Следующий результат даёт первый конструктивный способ построения из одной скрученной МП ЛРП целого класса скрученных МП ЛРП.

Теорема 3. *Пусть v — скрученная МП ЛРП порядка m над S с характеристическим многочленом*

$$\Psi(x) = x^m - \sum_{i=0}^{m-1} \psi_i x^i \in \check{S}[x], \quad \psi \in \check{S},$$

и $w = \psi(v)$ — последовательность элементов $w(i) = \psi\big(v(i)\big)$, $i \in \mathbb{N}_0$. Тогда

а) *если $\psi \in \check{S}^*$, то w — скрученная МП ЛРП с характеристическим многочленом*

$$\Psi'(x) = x^m - \sum_{i=0}^{m-1} (\psi \circ \psi_i \circ \psi^{-1}) x^i;$$

б) *если w — МП ЛРП над S, то $\psi \in \check{S}^*$.*

В терминах кольца матриц этот результат можно интерпретировать следующим образом. Если $v^{\downarrow}$ — последовательность векторов-столбцов $v^{\downarrow}(i) \in R^{(n)}$, удовлетворяющая некоторому закону рекурсии (1.8) и имеющая максимально возможный период τ, то для любой обратимой матрицы $U \in R^*_{n,n}$ последовательность $w^{\downarrow} = Uv^{\downarrow}$ также имеет период τ и удовлетворяет закону рекурсии

$$w^{\downarrow}(i+m) = (U^{-1}A_{m-1}U)w^{\downarrow}(i+m-1) + \ldots + (U^{-1}A_0U)w^{\downarrow}(i) \quad \text{для всех} \quad i \in \mathbb{N}_0. \tag{1.11}$$

В условиях пункта а) теоремы 3, если v — линейная рекуррента максимального периода порядка m над кольцом S, т. е. если $\Psi(x) \in S[x]$, назовём скрученную МП ЛРП $w = \psi(v)$ *линеаризуемой*.

Отметим, что в указанных выше работах скрученные МП ЛРП были найдены лишь в матричном виде над полями и с использованием методов перебора. Первый результат в этом направлении — скрученная МП ЛРП периода $2^{256} - 1$ и порядка 16 с «трёхчленным» законом рекурсии над модулем ${}_{\check{S}}S$, $S = \mathrm{GF}(2^{16})$, построенная в [10].

В [15, 16] анонсируются результаты полного перебора всех трёхчленных законов рекурсии порядка 8, генерирующих скрученные МП ЛРП над указанным модулем.

В [14] предлагается алгоритм построения скрученных МП ЛРП с характеристическим многочленом вида

$$\Psi(x) = x^m - \xi(s_{m-1}x^{m-1} - \ldots - s_1x - s_0),$$

где $\xi \in \check{S}$, $s_0, \dots s_{m-1} \in S$. Однако этот алгоритм предусматривает многократную проверку многочленов на неприводимость и вычисление порядков корней неприводимых многочленов.

Теорема 3 — первый из известных авторам результатов, позволяющих строить без использования метода перебора значительные классы скрученных МП ЛРП над конечными полями и кольцами Галуа, например класс линеаризуемых МП ЛРП.

Обозначим через $\mathrm{rk}_S v$, $\mathrm{rk}_R v$ ранг (степень минимального многочлена) последовательности $v \in S^{\langle 1 \rangle}$, рассматриваемой как ЛРП над модулями ${}_S S$ и ${}_R S$ соответственно (см. [9]). Из теоремы 2 следует, что для любой скрученной МП ЛРП v над кольцом S выполняется равенство $\mathrm{rk}_R v = mn$. Если v — обычная МП ЛРП над кольцом S, то по определению $\mathrm{rk}_S v = m$. В случае когда v — скрученная МП ЛРП над S, справедливы неравенства

$$m \leqslant \mathrm{rk}_S v \leqslant nm. \tag{1.12}$$

Интерес к скрученным МП ЛРП вызван прежде всего тем, что для них левое неравенство в (1.12) является строгим всегда, за исключением «тривиального» случая, когда v — обычная МП ЛРП над модулем ${}_S S$, а правое неравенство иногда достижимо.

Для того чтобы сформулировать общий результат, дающий нетривиальную нижнюю оценку параметра $\mathrm{rk}_S v$, заметим, что каждое линейное преобразование $\psi \in \check{S}$ модуля ${}_R S$ индуцирует линейное преобразование $\bar{\psi} \in \bar{\check{S}}$ пространства ${}_{\bar{R}} \bar{S}$ по правилу

$$\bar{\psi}(\bar{\alpha}) = \overline{\psi(\alpha)} \quad \text{для всех} \quad \alpha \in S.$$

Соответствие $\psi \to \bar{\psi}$ задаёт эпиморфизм колец $\check{S} \to \bar{\check{S}}$ с ядром $p\check{S}$, и канонический изоморфизм $\bar{\check{S}} \cong \check{S}/p\check{S}$ позволяет рассматривать $\bar{\psi}$ также как элемент фактор-кольца $\check{S}/p\check{S}$, т. е. использовать равенство $\bar{\psi} = \psi + p\check{S}$.

Теорема 4. *Пусть v — скрученная МП ЛРП порядка m над S с характеристическим многочленом*

$$\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x],$$

таким что

$$\bar{\Psi}(x) = x^m - \sum_{j=0}^{m-1} \bar{\psi}_j x^j \notin \bar{S}[x]. \tag{1.13}$$

Тогда

$$\mathrm{rk}_S v = km, \quad k \geqslant 2. \tag{1.14}$$

Ранг линеаризуемой МП ЛРП можно оценить точнее. Определим *вес* (*Хэмминга*) произвольного элемента

$$\psi = \sum_{l=0}^{n-1} s_l \sigma^l \in \check{S} \tag{1.15}$$

равенством

$$W(\psi) = |\{l \in \overline{0, n-1} \colon s_l \neq 0\}|.$$

Для произвольного многочлена

$$G(x) = \sum_{j \geqslant 0} g_j x^j \in S[x]$$

положим

$$\sigma\big(G(x)\big) = \sum_{j \geqslant 0} \sigma(g_j) x^j.$$

Теорема 5. *Пусть $u \in L_S\big(G(x)\big)$, где $G(x)$ — многочлен максимального периода над кольцом S степени m. Тогда последовательность $v = \psi(u)$ — скрученная МП ЛРП над S. При этом $\mathrm{rk}_S\, v = mW(\psi)$, а многочлен*

$$M(x) = \prod_{l \in \overline{0,n-1} \colon s_l \neq 0} \sigma^l\big(G(x)\big) \tag{1.16}$$

является минимальным многочленом ЛРП v над S.

Если $W(\psi) = n$, то $\mathrm{rk}_S\, v = \mathrm{rk}_R\, v = mn$ и $M(x)$ — многочлен максимального периода степени mn над кольцом R. Если к тому же преобразование (1.15) *удовлетворяет условию*

$$s_0, \ldots, s_{n-1} \in S^*, \tag{1.17}$$

то $M(x) \in R[x]$ — единственный минимальный многочлен ЛРП v над S.

В предыдущих работах не было теоретических результатов, посвящённых изучению рангов скрученных МП ЛРП как линейных рекуррент над модулем ${}_S S$. В [15, 16] приведены лишь результаты экспериментов, основанных на переборе, и отмечено, что ранг скрученной МП ЛРП порядка m может быть больше m, что интересно с точки зрения криптографии. Сформулированная теорема 4 указывает достижимую нижнюю границу ранга скрученной МП ЛРП в общем случае, а теорема 5 является конструктивной и позволяет точно находить ранг линеаризуемой скрученной МП ЛРП как линейной рекурренты над ${}_S S$ и строить скрученные МП ЛРП порядка m над модулем ${}_{\check{S}} S$, имеющие максимально возможный ранг mn над модулем ${}_S S$.

Мощность класса $\mathrm{LMP}_S(m)$ всех линеаризуемых многочленов максимального периода $\Psi(x) \in \check{S}[x]$ степени m можно подсчитать точно. Пусть $\mathrm{MP}_S(m)$ — множество всех многочленов максимального периода $G(x) \in S[x]$ степени m. Его мощность известна [6, 9, 13]:

$$|\mathrm{MP}_S(m)| = \begin{cases} \varphi(q^{nm} - 1)/m, & \text{если } d = 1, \\ (\varphi(q^{nm} - 1)/m)(q^{nm} - 1)q^{nm(d-2)}, & \text{если } d > 1 \text{ и } p > 2, \\ & \text{или } p = d = 2, \\ (\varphi(q^{nm} - 1)/m)(q^{nm} - 2)q^{nm(d-2)}, & \text{если } p = 2 < d. \end{cases} \tag{1.18}$$

Здесь и далее φ — функция Эйлера.

Теорема 6. *Множество* $\mathrm{LMP}_S(m)$ *имеет мощность*

$$|\mathrm{LMP}_S(m)| = \frac{|\mathrm{MP}_S(m)|}{n}\,\frac{|R^*_{n,n}|}{|S^*|}. \tag{1.19}$$

Окончательное числовое выражение для (1.19) получается с использованием (1.18) и известного равенства

$$|R^*_{n,n}| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})q^{(d-1)n^2}.$$

Следствие 7. *Если* $d=1$, *т. е.* $R=\mathrm{GF}(q)$, $S=\mathrm{GF}(q^n)$, *то*

$$|\mathrm{LMP}_S(m)| = \frac{\varphi(q^{nm}-1)}{nm}\,(q^n-q)\cdots(q^n-q^{n-1}). \tag{1.20}$$

В заключение этого раздела отметим, что в [15] выдвигается в качестве гипотезы эмпирически найденная формула, которая в наших терминах означает, что мощность множества $\mathrm{SMP}_S(m)$ всех скрученных многочленов максимального периода порядка m над полем $S=\mathrm{GF}(g^n)$ есть

$$|\mathrm{SMP}_S(m)| = \frac{\varphi(q^{nm}-1)}{nm}\,(q^n-q)\cdots\big(q^n-q^{(n-1)}\big)q^{n(n-1)(m-1)}. \tag{1.21}$$

Теоретически эта гипотеза доказана только в частных случаях: в [7] для $m=1$ и любого n, в [8] для $n=2$ и любого m.

Если эта гипотеза верна, то мы можем видеть, какова доля линеаризуемых МП ЛРП в множестве всех скрученных МП ЛРП:

$$|\mathrm{SMP}_S(m)| = |\mathrm{LMP}_S(m)|q^{n(n-1)(m-1)}.$$

2. Доказательство предложения 1

Пусть $v^{\downarrow}$ — последовательность векторов из $R^{(n)}$, удовлетворяющая некоторому закону рекурсии (1.8). Введём обозначения

$$\begin{aligned}
&\vec{v}(i) = \big(v_0(i), v_1(i), \ldots, v_{n-1}(i)\big) = \big(v^{\downarrow}(i)\big)^{\mathrm{T}},\\
&v^{\Downarrow}(i) = \Big(\vec{v}(i), \vec{v}\big(i+1\big), \ldots, \vec{v}\big(i+(m-1)\big)\Big)^{\mathrm{T}} =\\
&\quad = \big(v_0(i), \ldots, v_{n-1}(i), v_0(i+1), \ldots, v_{n-1}(i+1), \ldots,\\
&\quad v_0(i+m-1), \ldots, v_{n-1}(i+m-1)\big)^{\mathrm{T}}.
\end{aligned} \tag{2.1}$$

Тогда для матрицы

$$A = \begin{pmatrix}
0 & E & 0 & \ldots & 0\\
0 & 0 & E & \ldots & 0\\
\ldots & \ldots & \ldots & \ldots & \ldots\\
0 & 0 & 0 & \ldots & E\\
A_0 & A_1 & A_2 & \ldots & A_{m-1}
\end{pmatrix}_{mn\times mn} \tag{2.2}$$

над кольцом R справедливы равенства

$$Av^{\Downarrow}(i) = v^{\Downarrow}(i+1), \quad A^k v^{\Downarrow}(i) = v^{\Downarrow}(i+k), \quad k \in \mathbb{N}. \tag{2.3}$$

Пусть

$$F(x) = x^{mn} - f_{mn-1}x^{mn-1} - \ldots - f_1 x - f_0 = \chi_A(x) \in R[x] -$$

характеристический многочлен матрицы A. Тогда

$$A^{mn} = f_{mn-1}A^{mn-1} + \ldots + f_1 A + f_0 E.$$

Умножая обе части последнего равенства на $v^{\Downarrow}(i)$ и применяя (2.3), получаем

$$v^{\Downarrow}(i+mn) = f_{mn-1}v^{\Downarrow}(i+mn-1) + \ldots + f_0 v^{\Downarrow}(i), \quad i \in \mathbb{N}_0.$$

Ввиду (2.1) и (1.9) отсюда следуют равенства

$$\vec{v}(i+mn) = f_{mn-1}\vec{v}(i+mn-1) + \ldots + f_0\vec{v}(i), \quad i \in \mathbb{N}_0,$$
$$v(i+mn) = f_{mn-1}v(i+mn-1) + \ldots + f_0 v(i), \quad i \in \mathbb{N}_0.$$

Последние равенства означают, что $v \in L_S\big(F(x)\big)$. Из [6, 9] известно, что

$$T(v) \mid T(F) \leqslant (q^{mn}-1)p^{d-1}.$$

Предложение 1 доказано. □

3. Доказательство теоремы 2

Пусть последовательность $v \in S^{\langle 1\rangle}$ удовлетворяет некоторому закону рекурсии (1.4) и $T(v) = \tau$. Тогда так же, как и в доказательстве предложения 1, получаем, что $v \in L_S\big(F(x)\big)$, где $F(x)$ — характеристический многочлен матрицы A вида (2.2). Следовательно, $\tau = T(v) \mid T(F) \leqslant \tau$, и значит, $F(x)$ — многочлен максимального периода степени mn. Таким образом, соотношение (1.5) доказано.

Заметим теперь, что F — реверсивный многочлен и, значит, v — реверсивная последовательность. Отсюда следует, что если для последовательности v не выполняется условие (1.10), то ввиду (1.4) $v \in pS^{\langle 1\rangle}$. Однако в таком случае из (1.9) и (1.5) следует, что ввиду условия $F(x) \in R[x]$ для координатных последовательностей последовательности v выполняются условия

$$v_0, \ldots, v_{n-1} \in L_R(F), \tag{3.1}$$

$$v_0, \ldots, v_{n-1} \in pR^{\langle 1\rangle}. \tag{3.2}$$

Если $d = 1$, то последнее условие означает, что $v = 0$ и $T(v) = 1 < \tau$. Если $d > 1$, то из (3.1), (3.2) следует, что $T(v_k) \mid (p^{nm}-1)p^{d-2} < \tau$, $k \in \overline{0, n-1}$, и мы опять имеем противоречие с условием $T(v) = \tau$. Следовательно, условие (1.10) верно.

Пусть, наоборот, выполнены соотношения (1.10), (1.5). Покажем, что v есть скрученная МП ЛРП порядка m. Так как $F(x)$ — многочлен максимального

периода над R, то он имеет корень θ в расширении $K = GR(q^{nmd}, p^d)$ кольца S, причём $K = R[\theta]$ [13].

Так как все коэффициенты многочлена $F(x)$ принадлежат кольцу R, то каждая координатная последовательность v_k из разложения (1.9) последовательности v есть ЛРП над R с характеристическим многочленом $F(x)$. Следовательно, v_k представляется в виде

$$v_k(i) = \mathrm{Tr}_R^K(a_k\theta^i), \tag{3.3}$$

где Tr_R^K — след из кольца K в кольцо R, $a_k \in K$ [5, 13]. Покажем, что система элементов

$$\vec{\theta} = (a_0, \ldots, a_{n-1}, \ldots, a_0\theta^{m-1}, \ldots, a_{n-1}\theta^{m-1}) -$$

базис модуля ${}_RK$.

Допустим, что система $\vec{\theta}$ линейно зависима. Тогда существует элемент $\beta \in K^*$, такой что

$$\mathrm{Tr}_R^K(\beta\theta^{\downarrow}) \equiv 0^{\downarrow} \pmod{pR} \tag{3.4}$$

(здесь функция Tr применяется к вектору $\beta\theta^{\downarrow}$ покоординатно). Так как $\beta \in K^*$ и по условию элемент $\bar{\theta}$ порождает мультипликативную группу $\bar{K}^*$ поля вычетов $\bar{K} = \mathrm{GF}(q^{mn})$, то найдётся показатель $\delta_\beta \in \mathbb{N}_0$, такой что

$$\beta \equiv \theta^{\delta_\beta} \pmod{pK}. \tag{3.5}$$

Тогда для любых $k \in \overline{0, n-1}$, $j \in \overline{0, m-1}$, умножая (3.5) на $a_k\theta^j$, получаем

$$\beta a_k\theta^j \equiv \theta^{\delta_\beta} a_k\theta^j \pmod{pK},$$

и значит,

$$\mathrm{Tr}_R^K(\beta a_k\theta^j) \equiv \mathrm{Tr}_R^K(\theta^{\delta_\beta} a_k\theta^j) \pmod{pR}, \quad k \in \overline{0, n-1}, \quad j \in \overline{0, m-1}. \tag{3.6}$$

Ввиду (3.4) отсюда вытекает соотношение

$$\mathrm{Tr}_R^K(\theta^{\delta_\beta}\vec{\theta}) \equiv \mathrm{Tr}_R^K(\beta\vec{\theta}) \equiv \vec{0} \pmod{pR}.$$

Следовательно, для любого $k \in \overline{0, n-1}$

$$v_k(\,\overline{\delta_\beta, \delta_\beta + m - 1}\,) \in (pR)^m,$$

а тогда

$$v(\,\overline{\delta_\beta, \delta_\beta + m - 1}\,) \in (pS)^m,$$

что противоречит условию (1.10). Следовательно, $\vec{\theta}$ — базис модуля ${}_RK$.

В таком случае система $\vec{\theta_1} = \theta \cdot \vec{\theta}$ линейно выражается через $\vec{\theta}$, т. е. существует матрица $B \in R_{mn,mn}$, такая что

$$B\theta^{\downarrow} = \theta_1^{\downarrow}.$$

Следовательно, для любого $j \in \mathbb{N}_0$

$$B \cdot \mathrm{Tr}_R^K(\theta^j\theta^{\downarrow}) = \mathrm{Tr}_R^K(\theta^j\theta_1^{\downarrow}) = \mathrm{Tr}_R^K(\theta^{j+1}\theta^{\downarrow}).$$

Отсюда получаем равенство

$$B\big(v_0(j),\dots,v_{n-1}(j),\dots,v_0(m-1+j),\dots,v_{n-1}(m-1+j)\big)^{\mathrm{T}} = \\ = \big(v_0(j+1),\dots,v_{n-1}(j+1),\dots,v_0(m+j),\dots,v_{n-1}(m+j)\big)^{\mathrm{T}},$$

или в обозначениях (2.1)

$$Bv^{\Downarrow}(i) = v^{\Downarrow}(i+1). \tag{3.7}$$

Пусть матрицы $A_0,\dots,A_{m-1}\in R_{n,n}$ определяются из равенства

$$(A_0,\dots,A_{m-1}) = \begin{pmatrix} \vec{B}_{(m-1)n+1} \\ \dots \\ \vec{B}_{mn} \end{pmatrix},$$

где в правой части стоит матрица, составленная из последних n строк матрицы B. Тогда из (3.7) следует, что

$$(A_0,A_1,\dots,A_{m-1}) \begin{pmatrix} v^{\downarrow}(j) \\ v^{\downarrow}(j+1) \\ \dots \\ v^{\downarrow}(j+m-1) \end{pmatrix} = v^{\downarrow}(j+m),$$

т. е.

$$v^{\downarrow}(j+m) = A_0v^{\downarrow}(j) + \ldots + A_{m-1}v^{\downarrow}(j+m-1). \tag{3.8}$$

Следовательно, v — скрученная ЛРП порядка m периода τ.

Для доказательства последнего утверждения теоремы остаётся заметить, что так как $\vec{\theta}$ — базис модуля ${}_RK$, то система коэффициентов $a_0,\dots,a_{n-1}\in K$ линейно независима над R и, в частности, $a_k\in K^*$, $k\in\overline{0,n-1}$. Теперь из (3.3) следует, что система последовательностей $v_0,\dots,v_{n-1}$ есть система МП ЛРП с минимальным многочленом $F(x)$, линейно независимая над R (а значит, и над любым расширением кольца R). □

4. Доказательство теоремы 3

Докажем утверждение а). Если $\psi\in\check{S}^*$, то, очевидно, $T(w)=T(v)=\tau$. Остаётся доказать, что w — скрученная ЛРП порядка m с характеристическим многочленом $\Psi'(x)$. Так как последовательность v удовлетворяет условиям (1.4), то

$$\psi\big(v(i+m)\big) = \psi\Big(\psi_{m-1}\big(v(i+m-1)\big)\Big) + \ldots + \psi\Big(\psi_0\big(v(i)\big)\Big) \quad \text{для всех} \quad i\in\mathbb{N}_0.$$

Эти соотношения можно также представить в виде

$$\psi\big(v(i+m)\big) = \psi\circ\psi_{m-1}\circ\psi^{-1}\Big(\psi\big(v(i+m-1)\big)\Big) + \ldots + \\ + \psi\circ\psi_0\circ\psi^{-1}\Big(\psi\big(v(i)\big)\Big) \quad \text{для всех} \quad i\in\mathbb{N}_0,$$

или

$$w(i+m) = \psi \circ \psi_{m-1} \circ \psi^{-1}\big(w(i+m-1)\big) + \ldots + \psi \circ \psi_0 \circ \psi^{-1}\big(w(i)\big) \quad \text{для всех} \quad i \in \mathbb{N}_0.$$

Таким образом, $w \in L_S\big(\Psi'(x)\big)$.

Докажем утверждение б). Допустим, что ψ не является обратимым элементом кольца $\check{S}$. Тогда система строк матрицы $A(\psi)$ линейно зависима. Учитывая равенство

$$w^{\downarrow}(\overline{0, \tau-1}) = A(\psi) v^{\downarrow}(\overline{0, \tau-1}),$$

получаем, что система координатных последовательностей $w_0, \ldots, w_{n-1}$ также линейно зависима над R, а тогда из теоремы 2 следует, что w не является скрученной ЛРП максимального периода. □

5. Доказательство теоремы 4

Как уже отмечалось, из теоремы 2 следует, что

$$v = \sum_{k=0}^{n-1} v_k \alpha_k,$$

где $v_0, \ldots, v_{n-1} \in L_R(F)$ для некоторого многочлена максимального периода $F(x) \in R[x]$ степени mn. Следовательно, $v \in L_S\big(F(x)\big)$. При этом, согласно [9], многочлен $\bar{F}(x)$ является многочленом максимального периода над полем $\bar{R}$. Известно [11], что $\bar{F}(x)$ раскладывается над расширением $\bar{S}$ поля $\bar{R}$ в произведение n различных унитарных неприводимых сомножителей степени m каждый:

$$\bar{F}(x) = g_1(x) \cdot \ldots \cdot g_n(x).$$

По лемме Гензеля [5, 9, 13] последнее разложение однозначно поднимается до разложения в $S[x]$:

$$F(x) = G_1(x) \cdot \ldots \cdot G_n(x), \quad G_i(x) \in S[x], \quad \bar{G}_i(x) = g_i(x), \quad i \in \overline{1, n}. \tag{5.1}$$

Так как сомножители в этом разложении попарно взаимно просты, то справедливо равенство

$$L_S(F) = L_S(G_1) \dotplus \ldots \dotplus L_S(G_n), \tag{5.2}$$

ввиду которого последовательность v однозначно представляется в виде суммы

$$v = v^{(1)} + \ldots + v^{(n)}, \quad v^{(t)} \in L_S(G_t), \quad t \in \overline{1, n}. \tag{5.3}$$

Минимальный многочлен $M(x)$ рекурренты v над S есть унитарный многочлен наименьшей возможной степени из $S[x]$ со свойством

$$M(x)v = 0. \tag{5.4}$$

Такой многочлен определяется, вообще говоря, не однозначно, однако однозначно определяется его образ $\bar{M}(x)$ над полем $\bar{S}$ и, в частности, степень:

$\deg M(x) = \deg \bar{M}(x) = \operatorname{rk} v$ [5, 9, 13]. Для описания многочлена $\bar{M}(x)$ в рассматриваемой ситуации докажем несколько более общее утверждение, которое окажется полезным и далее.

Мы называем унитарный многочлен $G(x) \in S[x]$ *многочленом Галуа* [4, 13], если $\bar{G}(x)$ — неприводимый многочлен над $\bar{S}$.

Лемма 8. *Пусть многочлен $F(x) \in S[x]$ есть произведение* (5.1) *попарно взаимно простых многочленов Галуа, и пусть $v^{(i_1)}, \ldots, v^{(i_k)}$ — все ненулевые ЛРП из разложения* (5.3) *последовательности $v \in L_S(F)$. Тогда многочлен*

$$M(x) = G_{i_1}(x) \cdot \ldots \cdot G_{i_k}(x) \tag{5.5}$$

является минимальным многочленом ЛРП v. Любой минимальный многочлен $M(x)$ указанной ЛРП удовлетворяет условию

$$\bar{M}(x) = g_{i_1}(x) \cdot \ldots \cdot g_{i_k}(x). \tag{5.6}$$

Если в разложении (5.3) $\bar{v}^{(l)} \neq \bar{0}$ *для $l \in \overline{1,n}$, то ЛРП v имеет единственный минимальный многочлен*:

$$M(x) = G_1(x) \cdot \ldots \cdot G_n(x). \tag{5.7}$$

Доказательство. Согласно [5] многочлен $M(x)$ можно определить также как главный образующий идеала

$$\operatorname{An}_{S[x]}(v) = \{A(x) \in S[x] \colon A(x)v = 0\},$$

т. е. унитарный многочлен, удовлетворяющий условию

$$\operatorname{An}_{S[x]}(v) = S[x]M(x) + pS[x] \cap \operatorname{An}_{S[x]}(v).$$

Ввиду неприводимости над $\bar{S}$ каждого из многочленов $\bar{G}_{i_r}(x) = g_{i_r}(x)$, $r \in \overline{1,k}$, из условия (5.3) следует, что справедливы равенства

$$\operatorname{An}_{S[x]}\bigl(v^{(i_r)}\bigr) = S[x]G_{i_r}(x) + p^{d-d_r}S[x], \quad r \in \overline{1,k}, \tag{5.8}$$

где

$$d_r = \bigl\|v^{(i_r)}\bigr\| = \max\bigl\{\delta \in \overline{0,d} \colon v^{(i_r)} \in p^\delta S^{\langle 1\rangle}\bigr\} -$$

норма последовательности $v^{(i_r)}$.

При сделанных предположениях из (5.3) следует равенство

$$\operatorname{An}_{S[x]}(v) = \bigcap_{r\in\overline{1,k}} \operatorname{An}_{S[x]}\bigl(v^{(i_r)}\bigr)$$

и, так как ввиду (5.8) идеалы в правой части этого равенства попарно комаксимальны, равенство

$$\operatorname{An}_{S[x]}(v) = \prod_{r\in\overline{1,k}} \operatorname{An}_{S[x]}\bigl(v^{(i_r)}\bigr). \tag{5.9}$$

Отсюда по (5.8) следует, что многочлен (5.5) — один из главных образующих идеала $\operatorname{An}_{S[x]}(v)$, т. е. минимальный многочлен ЛРП v. Следовательно, справедливо равенство (5.6).

Условие $\bar{v}^{(l)} \neq \bar{0}$, $l \in \overline{1,n}$, означает, что $k = n$ и равенства (5.8), (5.9) обращаются в равенства

$$\mathrm{An}_{S[x]}\big(v^{(l)}\big) = S[x]G_l(x), \quad l \in \overline{1,n}, \quad \mathrm{An}_{S[x]}(v) = \prod_{l \in \overline{1,n}} S[x]G_l(x).$$

Этим доказано последнее утверждение леммы. □

Таким образом, если параметр k определяется из условия леммы 8, то $\mathrm{rk}\, v = \deg \bar{M}(x) = mk$.

Покажем, что при условии (1.13) равенство $\mathrm{rk}\, v = m$ невозможно, т. е. $k > 1$.

Допустим, что $k = 1$. Тогда $v = v^{(i_1)}$ есть МП ЛРП над S с характеристическим многочленом $G_{i_1}(x)$ и $\bar{v}$ есть МП ЛРП над полем $\bar{S}$ с минимальным многочленом

$$\bar{G}_{i_1}(x) = g_{i_1}(x) = x^m - h_{m-1}x^{m-1} - \ldots - h_1 x - h_0 \in \bar{S}[x].$$

В таком случае ввиду (1.2) последовательность $\bar{v}$ аннулируется многочленом

$$\delta(x) = \sum_{t \in \overline{0,m-1}} (\bar{\psi}_t - h_t)x^t \in \check{\bar{S}}[x], \tag{5.10}$$

причём $\delta(x) \neq \bar{0}$, так как по условию (1.13) теоремы $\bar{\psi}_t \notin \bar{S}$ для некоторого $t \in \overline{0, m-1}$. Это невозможно, так как справедлива следующая лемма.

Лемма 9. *Если $\bar{v}$ есть МП ЛРП ранга m над полем $\bar{S}$ с минимальным многочленом $g(x) \in \bar{S}[x]$, то*

$$\mathrm{An}_{\check{\bar{S}}[x]}(\bar{v}) = \check{\bar{S}}[x]g(x).$$

Доказательство. Деля в кольце $\check{\bar{S}}[x]$ произвольный многочлен $f(x) \in \in \mathrm{An}_{\check{\bar{S}}[x]}(\bar{v})$ с остатком справа на $g(x)$, получаем

$$f(x) = a(x)g(x) + \rho(x), \quad \deg \rho(x) < m, \quad \rho(x)\bar{v} = \bar{0}.$$

Если $\rho(x) \neq 0$, то последние два соотношения невозможны, так как ввиду условия на $\bar{v}$ для некоторого $i \in \mathbb{N}_0$ выполняется равенство $\bar{v}[\overline{i, i+m-1}] = = (0, \ldots, 0, e)$. □

Теорема 4 доказана. □

6. Доказательство теоремы 5

Рассмотрим p-адическое координатное множество кольца Галуа S:

$$\Gamma(S) = \big\{s \in S\colon s^{|\bar{S}|} = s\big\} = \big\{s \in S\colon s^{q^n} = s\big\}.$$

Оно имеет мощность $q^n = |\bar{S}|$ и удовлетворяет условию $\bar{\Gamma}(S) = \bar{S}$. При этом каждый элемент $s \in S$ однозначно представляется в виде суммы

$$s = \gamma_0(s) + p\gamma_1(s) + \ldots + p^{n-1}\gamma_{n-1}(s), \quad \gamma_0(s), \ldots, \gamma_{n-1}(s) \in \Gamma(S), \tag{6.1}$$

называемой *p-адическим разложением элемента* s. При таком представлении автоморфизм σ, порождающий группу $\mathrm{Aut}(S/R)$, может быть задан следующим образом:

$$\sigma(s) = \gamma_0(s)^q + p\gamma_1(s)^q + \ldots + p^{n-1}\gamma_{n-1}(s)^q.$$

Этот автоморфизм называется *автоморфизмом Фробениуса* S над R.

Пусть теперь K — расширение Галуа кольца S степени m из раздела 3. Тогда p-адическое координатное множество $\Gamma(S)$ есть подполугруппа полугруппы $(\Gamma(K), \cdot)$, каждый элемент $\alpha \in K$ имеет разложение

$$\alpha = \gamma_0(\alpha) + p\gamma_1(\alpha) + \ldots + p^{n-1}\gamma_{n-1}(\alpha), \quad \gamma_0(\alpha), \ldots, \gamma_{n-1}(\alpha) \in \Gamma(K), \tag{6.2}$$

и автоморфизм Фробениуса $\varkappa \in \mathrm{Aut}(K/R)$ имеет вид

$$\varkappa(\alpha) = \gamma_0(\alpha)^q + p\gamma_1(\alpha)^q + \ldots + p^{n-1}\gamma_{n-1}(\alpha)^q, \tag{6.3}$$

а автоморфизм Фробениуса K над S есть $\varkappa^n$. Очевидно, ограничение $\varkappa|S$ автоморфизма $\varkappa$ на подкольцо S есть σ:

$$\varkappa|S = \sigma. \tag{6.4}$$

Переходим к доказательству теоремы 5. Пусть $\theta \in K$ — корень многочлена $G(x)$. Тогда для некоторого $\xi \in K^*$

$$u(i) = \mathrm{Tr}_S^K(\xi\theta^i) = \sum_{t \in \overline{0,m-1}} \varkappa^{nt}(\xi\theta^i), \quad i \in \mathbb{N}_0, \tag{6.5}$$

и при условии (1.15) последовательность $v = \psi(u)$, с учётом (6.4), имеет вид

$$\begin{aligned} v(i) &= \sum_{l \in \overline{0,n-1}} s_l \sigma^l\big(u(i)\big) = \sum_{l \in \overline{0,n-1}} s_l \varkappa^l\big(u(i)\big) = \\ &= \sum_{l \in \overline{0,n-1}} s_l \sum_{t \in \overline{0,m-1}} \varkappa^{nt}\big(\varkappa^l(\xi)\big(\varkappa^l(\theta)\big)^i\big) = \sum_{l \in \overline{0,n-1}} s_l \,\mathrm{Tr}_S^K\big(\varkappa^l(\xi)\big(\varkappa^l(\theta)\big)^i\big). \end{aligned} \tag{6.6}$$

Для каждого $l \in \overline{0, n-1}$ элемент $\varkappa^l(\xi)$ обратим в K, и последовательность $u^{(l)}$ элементов

$$u^{(l)}(i) = \mathrm{Tr}_S^K\big(\varkappa^l(\xi)\big(\varkappa^l(\theta)\big)^i\big)$$

есть МП ЛРП с минимальным многочленом

$$G_l(x) = \prod_{t \in \overline{0,m-1}} \Big(x - \varkappa^{nt}\big(\varkappa^l(\theta)\big)\Big) = \varkappa^l\Big(\prod_{t \in \overline{0,m-1}} \big(x - \varkappa^{nt}(\theta)\big)\Big) = \varkappa^l\big(G(x)\big). \tag{6.7}$$

Ввиду (6.4) отсюда следуют соотношения

$$G_l(x) = \sigma^l\big(G(x)\big), \quad l \in \overline{0, n-1}. \tag{6.8}$$

Лемма 10. *Многочлены $G_0(x), \ldots, G_{n-1}(x)$ попарно взаимно просты.*

Доказательство. Достаточно заметить, что если $t, t' \in \overline{0, m-1}$, $l, l' \in \overline{0, n-1}$ и $(t, l) \neq (t', l')$, то разность элементов $\varkappa^{nt}\big(\varkappa^{l}(\theta)\big) = \varkappa^{nt+l}(\theta)$ и $\varkappa^{nt'}\big(\varkappa^{l'}(\theta)\big) = \varkappa^{nt'+l'}(\theta)$ — обратимый элемент кольца K, поскольку $\bar{\theta}$ — примитивный элемент поля $\bar{K}$. Следовательно, многочлены $x - \varkappa^{nt}\big(\varkappa^{l}(\theta)\big)$ и $x - \varkappa^{nt'}\big(\varkappa^{l'}(\theta)\big)$ взаимно просты. Ввиду (6.7) отсюда следует, что если $l \neq l'$, то многочлены $G_l(x)$ и $G_{l'}(x)$ взаимно просты. □

Последовательность $v^{(l)} = s_l u^{(l)}$ принадлежит семейству $L_S(G_l)$ и имеет норму $\|v^{(l)}\| = \|s_l\|$.

Теперь из (6.6) следует равенство

$$v = v^{(0)} + \ldots + v^{(n-1)}, \quad v^{(l)} \in L_S(G_l), \quad l \in \overline{0, n-1}, \tag{6.9}$$

причём число ненулевых слагаемых в этом разложении равно, очевидно, $W(\psi)$. Остаётся заметить, что так как по лемме 10 $G_0(x), \ldots, G_{n-1}(x)$ — система попарно взаимно простых многочленов Галуа, то нужные свойства последовательности v следуют из леммы 8. Теорема 5 доказана. □

7. Доказательство теоремы 6

Для произвольного элемента $s \in S$ обозначим через $\hat{s}$ линейное преобразование модуля ${}_RS$ по правилу $\hat{s}(x) = sx$ (гомотетию). Для любого обратимого элемента $\psi \in \check{S}$ введём обозначение

$$s^{\psi} = \psi \circ \hat{s} \circ \psi^{-1} \in \check{S},$$

и для любого унитарного многочлена

$$G(x) = x^m - \sum_{k \in \overline{0, m-1}} g_k x^k \in S[x]$$

положим

$$G^{\psi}(x) = x^m - \sum_{k \in \overline{0, m-1}} g_k^{\psi} x^k \in \check{S}[x].$$

Тогда изучаемое множество $\mathrm{LMP}_S(m)$ есть множество всех различных многочленов вида

$$G^{\psi}(x), \quad \text{где} \quad G(x) \in \mathrm{MP}_S(m), \quad \psi \in \check{S}^*. \tag{7.1}$$

Для подсчёта мощности этого множества докажем несколько вспомогательных утверждений.

Лемма 11. *Свободный член g_0 многочлена $G(x) \in \mathrm{MP}_S(m)$ порождает кольцо S над R:*

$$S = R[g_0]. \tag{7.2}$$

Доказательство. Пусть θ — корень $G(x)$ в расширении Галуа K кольца S степени m. Тогда в обозначениях из доказательства предыдущей теоремы

$$G(x) = \prod_{t \in \overline{0, m-1}} \big(x - \varkappa^{nt}(\theta)\big), \tag{7.3}$$

откуда следует, что

$$g_0 = (-1)^m \prod_{t\in\overline{0,m-1}} \varkappa^{nt}(\theta),$$

и ввиду (6.3)

$$\bar{g}_0 = (-1)^m \bar{\theta}^{\Delta}, \quad \Delta = \frac{q^{nm}-1}{q^n-1}.$$

Так как $\bar{\theta}^{\Delta} = (-1)^m \bar{g}_0$ — примитивный элемент поля $\bar{S}$, то, очевидно, $\bar{S} = \bar{R}[\bar{g}_0]$. Последнее равенство равносильно (7.2) [4]. □

Напомним, что *централизатором* элемента $w \in \check{S}^*$ в группе $\check{S}^*$ называется её подгруппа

$$\mathrm{Z}_{\check{S}^*}(w) = \{\psi \in \check{S}^* \colon \psi w = w\psi\}.$$

Лемма 12. *Если* $G(x) \in \mathrm{MP}_S(m)$, *то* $\mathrm{Z}_{\check{S}^*}(g_0) = S^*$.

Доказательство. Пользуясь изоморфизмами (1.1), отождествим каждый элемент $\psi \in \check{S}$ с матрицей $A(\psi) \in R_{n,n}$ линейного преобразования ψ в фиксированном выше базисе $\vec{\alpha}$ модуля ${}_RS$ (см. раздел 1). Заметим, что согласно (7.2) элемент g_0 — корень многочлена Галуа $f(x) \in R[x]$ степени n [4,13]. Тогда матрица $A(\hat{g}_0)$ также аннулируется этим многочленом, и ввиду неприводимости многочлена $\bar{f}(x) \in \bar{R}[x]$ последний является одновременно минимальным и характеристическим многочленом матрицы $\bar{A}(\hat{g}_0)$. В таком случае, как показано в [6], с матрицей $A(\hat{g}_0)$ перестановочны лишь те матрицы из $R_{n,n}$, которые представляются в виде $c\big(A(\hat{g}_0)\big)$, $c(x) \in R[x]$. Это означает, что с элементом g_0 перестановочны те и только те элементы $\psi \in \check{S}$, которые представляются в виде $\psi = c(g_0)$, $c(x) \in R[x]$, т. е. ввиду (7.2) в точности все элементы кольца S. □

Для фиксированного многочлена $G(x) \in \mathrm{MP}_S(m)$ обозначим через $\mathrm{LMP}_S(G)$ множество всех различных многочленов из набора $G^{\psi}(x)$, $\psi \in \check{S}^*$.

Лемма 13. *Пусть* $G(x) \in \mathrm{MP}_S(m)$. *Тогда*

$$|\mathrm{LMP}_S(G)| = \frac{|R^*_{n,n}|}{|S^*|}.$$

Доказательство. Согласно (7.2) все коэффициенты многочлена $G(x)$ принадлежат кольцу $R[g_0]$. Поэтому согласно лемме 12 для любого $\psi \in \check{S}^*$ $G^{\psi}(x) = G(x)$ тогда и только тогда, когда $\psi \in \mathrm{Z}_{\check{S}^*}(g_0) = S^*$. Следовательно, число $|\mathrm{LMP}_S(G)|$ равно индексу подгруппы S^* в группе $\check{S}^*$. □

Множество $\mathrm{LMP}_S(m)$ всех различных многочленов из набора (7.1) можно представить в виде

$$\mathrm{LMP}_S(m) = \bigcup_{G\in\mathrm{MP}(m)} \mathrm{LMP}(G). \tag{7.4}$$

С учётом последней леммы ясно, что для подсчёта мощности множества в левой части равенства (7.4) достаточно доказать, что множества в его правой части либо не пересекаются, либо совпадают, и найти количество различных множеств.

Лемма 14. *Для любых многочленов* $G(x), H(x) \in \mathrm{MP}_S(m)$ *следующие утверждения равносильны*:

а) $\mathrm{LMP}(G) \cap \mathrm{LMP}(H) \neq \varnothing$;

б) $\mathrm{LMP}(G) = \mathrm{LMP}(H)$;

в) $H(x) = G^{\sigma^l}(x)$, *где* $l \in \overline{0, n-1}$.

Доказательство. Докажем импликацию а) $\Longrightarrow$ б). Для любого $\xi \in \check{S}^*$ множество всех различных многочленов из совокупности $G^{\xi\circ\psi}(x)$, $\psi \in \check{S}^*$, совпадает с $\mathrm{LMP}(G)$. Следовательно, если для некоторых $\xi, \eta \in \check{S}*$ выполняется условие

$$G^{\xi}(x) = H^{\eta}(x) \in \mathrm{LMP}(G) \cap \mathrm{LMP}(H),$$

то справедливо б).

Докажем импликацию б) $\Longrightarrow$ в). Из условия б) следует, что $H(x) = G^{\psi}(x)$ для некоторого $\psi \in \check{S}^*$. Следовательно, $g_0^{\psi} \in S$, и ввиду (7.2) отображение $\delta\colon S \to \check{S}$, определённое по правилу $\delta(s) = s^{\psi}$, есть отображение $\delta\colon S \to S$ и автоморфизм кольца S над R, т. е. $\delta = \sigma^l$ для некоторого $l \in \overline{0, n-1}$. Это означает, что разложение (1.15) элемента ψ имеет вид $\psi = s_l\sigma^l$, $s_l \in S^*$, и потому $H(x) = G^{\psi}(x) = G^{\sigma^l}(x)$.

Импликация в) $\Longrightarrow$ а) очевидна. □

Теперь очевидно, что правая часть равенства (7.4) есть объединение $|MP_S(m)|/n$ попарно не пересекающихся множеств, каждое из которых по лемме 13 имеет мощность $|R^*_{n,n}|/|S^*|$. Теорема 6 доказана. □

Литература

[1] Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. Т. 2. — М.: Гелиос АРВ, 2003.

[2] Куракин В. Л. Алгоритм Берлекэмпа—Месси над конечными кольцами, модулями и бимодулями // Дискрет. мат. — 1998. — Т. 10, № 4. — С. 3—34.

[3] Нечаев А. А. Конечные кольца главных идеалов // Мат. сб. — 1973. — Т. 91, № 3. — С. 350—366.

[4] Нечаев А. А. Код Кердока в циклической форме // Дискрет. мат. — 1989. — Т. 1, № 4. — С. 123—139.

[5] Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами // Дискрет. мат. — 1991. — Т. 3, № 4. — С. 107—121.

[6] Нечаев А. А. Цикловые типы линейных подстановок над конечными коммутативными кольцами // Мат. сб. — 1993. — Т. 184, № 3. — С. 21—56.

[7] Ghorpade S. R., Hasan S. U., Kumari M. Primitive polynomials, Singer cycles, and word-oriented linear feedback shift registers // Des. Codes Cryptogr. — 2011. — Vol. 58, no. 2. — P. 123—134.

[8] Ghorpade S. R., Ram S. Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields // Finite Fields Appl. — 2011. — Vol. 17, no. 5. — P. 461—472.

[9] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. — 1995. — Vol. 76, no. 6. — P. 2793—2915.

[10] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyschev V. N. Linear and polylinear recurring sequences over Abelian groups and modules // J. Math. Sci. — 2000. — Vol. 102, no. 6. — P. 4598—4626.

[11] Lidl R., Niederreiter H. Finite Fields. — Cambridge: Cambridge Univ. Press, 1983. — (Encyclopedia of Mathematics and Its Applications; Vol. 20).

[12] McDonald B. R. Finite Rings with Identity. — New York: Marcel Dekker, 1974.

[13] Nechaev A. A. Finite rings with applications // Handbook of Algebra. Vol. 5 / M. Hazewinkel, ed. — Elsevier, 2008. — P. 213—320.

[14] Tsaban B., Vishne U. Efficient linear feedback shift registers with maximal period // Finite Fields Appl. — 2002. — Vol. 8, no. 2. — P. 256—267.

[15] Zeng G., Han W., He K. Word-oriented feedback shift register: σ-LFSR. — Cryptology ePrint Archive: Report 2007/114. — `http://eprint.iacr.org/2007/114`.

[16] Zeng G., He K. C., Han W. A trinomial type of σ-LFSR oriented toward software implementation // Sci. China. Ser. F Information Sci. — 2007. — Vol. 50, no. 3. — P. 359—372.

[17] Zeng G., Yang Y., Han W., Fan S. Word oriented cascade jump σ-LFSR // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. 18th Int. Symp., AAECC-18, Tarragona, Sapin, June 8—12, 2009. Proceedings / M. Bras-Amorós, ed. — Berlin: Springer, 2009. — (Lect. Notes Comput. Sci.; Vol. 5527). — P. 127—136.