Math-Net.Ru

Общероссийский математический портал

М. А. Гольтваница, Новые представления знаков скрученных ЛРП при помощи функции след, базирующиеся на некоммутативной теореме Гамильтона – Кэли, *Матем. вопр. криптогр.*, 2021, том 12, выпуск 1, 23–57

DOI: <https://doi.org/10.4213/mvk347>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.187.58

26 апреля 2023 г., 17:27:18

Новые представления знаков скрученных ЛРП при помощи функции след, базирующиеся на некоммутативной теореме Гамильтона – Кэли

М. А. Гольтованица

ООО «Центр сертификационных исследований», Москва

Получено 15.V.2020

Аннотация. Пусть p — простое число, $R = \text{GR}(q^d, p^d)$ — кольцо Галуа мощности q^d и характеристики p^d , где $q = p^r$, $S = \text{GR}(q^{nd}, p^d)$ — расширение степени n кольца R , а $\text{End}({}_R S)$ — кольцо эндоморфизмов модуля ${}_R S$. Последовательность v над S , удовлетворяющая закону рекурсии

$$\forall i \in \mathbb{N}_0: v(i+m) = \psi_{m-1}(v(i+m-1)) + \dots + \psi_0(v(i)),$$

$\psi_0, \dots, \psi_{m-1} \in \text{End}({}_R S)$, называется *скрученной линейной рекуррентной последовательностью (ЛРП) над S* ; ее максимально возможный период равен $(q^{mn} - 1)p^{d-1}$. С использованием функции след для представлений элементов скрученной ЛРП максимального периода доказано, что такая ЛРП линеаризуема, если коэффициенты в законе рекурсии попарно коммутируют.

Ключевые слова: кольцо Галуа, автоморфизм Фробениуса, последовательность максимального периода, скрученная ЛРП, функция след

New representaions of elements of skew linear recurrent sequences via trace function based on the noncommutative Hamilton – Cayley theorem

M. A. Goltvanitsa

LLC «Certification Research Center», Moscow

Abstract. Let p be a prime number, $R = \text{GR}(q^d, p^d)$ be a Galois ring of cardinality q^d and characteristic p^d , where $q = p^r$, $S = \text{GR}(q^{nd}, p^d)$ be its extension of degree n and $\text{End}({}_R S)$ be a ring of endomorphisms of the module ${}_R S$. A sequence v over S satisfying a recursion law

$$\forall i \in \mathbb{N}_0: v(i+m) = \psi_{m-1}(v(i+m-1)) + \dots + \psi_0(v(i)),$$

$\psi_0, \dots, \psi_{m-1} \in \text{End}({}_R S)$, is called *skew linear recurrent sequence (LRS) over S* ; the maximal period of such sequence is equal to $(q^{mn} - 1)p^{d-1}$. Using the trace function for representations of elements of skew LRS of maximal period we show that such LRS may be linearized if the coefficients in the recursion law are pairwise commuting.

Keywords: Galois ring, Frobenius automorphism, ML-sequence, skew LRS, trace function

1. Введение. Основные результаты

Далее $R = \text{GR}(q^d, p^d)$ — кольцо Галуа мощности q^d и характеристики p^d , где $q = p^r$, p — простое число, $S = \text{GR}(q^{nd}, p^d)$ — расширение Галуа степени n кольца R [1]. Известно, что группа $\text{Aut}(S/R)$ автоморфизмов кольца S над R — циклическая порядка n [2]. Пусть σ — образующий элемент этой группы и $\check{S} = S^\sigma \langle \sigma \rangle$ — скрученное групповое кольцо группы $\langle \sigma \rangle$ над S , т. е. кольцо $\check{S}$ есть множество всевозможных формальных сумм вида

$$\psi = \sum_{j=0}^{n-1} s_j \sigma^j, \quad s_0, \dots, s_{n-1} \in S,$$

с естественным сложением и умножением, определяемым дистрибутивностью и тождеством

$$\forall s \in S: \sigma s = \sigma(s) \sigma.$$

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

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

обратно, каждый эндоморфизм R -модуля ${}_R S$ имеет такой вид. Поэтому существуют изоморфизмы

$$\check{S} \cong \text{End}({}_R S) \cong R_{n,n}, \quad (1)$$

где $R_{n,n}$ — кольцо $n \times n$ -матриц над R . Далее мы отождествляем элементы из $\check{S}$ с соответствующими элементами из $\text{End}({}_R S)$.

Определим на S структуру левого $\check{S}$ -модуля:

$$\psi \circ s = \psi(s). \quad (2)$$

При таком определении множество $S^{(1)}$ последовательностей над S есть левый модуль над кольцом многочленов $\check{S}[x]$, в котором умножение последовательности $v \in S^{(1)}$ на многочлен $A(x) = \sum_{j \geq 0} a_j x^j \in \check{S}[x]$ задается равенством

$$A(x)v = w \in S^{(1)} : w(i) = \sum_{j \geq 0} a_j (v(i+j)), \quad i \geq 0.$$

Следуя [3], последовательность $v \in S^{(1)}$ назовем *скрученной линейной рекуррентной последовательностью (ЛРП)* порядка $m > 0$ над кольцом S , если v есть ЛРП порядка m над модулем ${}_S S$ [1, 4], т.е. если равенство $\Psi(x)v = 0$ справедливо для некоторого унитарного многочлена

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \dots - \psi_0 \in \check{S}[x] \quad (3)$$

степени m , называемого *характеристическим многочленом ЛРП* v , или, что то же самое, если последовательность v удовлетворяет закону рекурсии

$$\forall i \in \mathbb{N}_0 \quad v(i+m) = \psi_{m-1}(v(i+m-1)) + \dots + \psi_0(v(i)). \quad (4)$$

Обозначим через $L_S(\Psi)$ множество всех ЛРП v над S с характеристическим многочленом $\Psi(x)$. Если $\Psi(x) \in S[x]$, то многочлен $\Psi(x)$ и последовательности из семейства $L_S(\Psi)$ будем называть *классическими*. Далее мы используем стандартное обозначение $T(v)$ для минимального периода периодической последовательности v над S . Аналогичное обозначение используется для периодов унитарных многочленов.

Предложение 1 ([3]). *Для любой скрученной ЛРП v порядка m над S существует такой унитарный многочлен $F(x) \in R[x]$ степени mn , что*

$$v \in L_S(F). \quad (5)$$

При этом справедливы соотношения

$$T(v)|T(F), \quad T(F) \leq \tau = (q^{mn} - 1)p^{d-1}. \quad (6)$$

Если в условиях предложения 1 выполнено равенство

$$T(v) = \tau,$$

то последовательность v будем называть *скрученной ЛРП максимального периода (МП ЛРП)*. Унитарный многочлен $\Psi(x)$ над $\check{S}$

степени m будем называть *многочленом максимального периода* (МП-многочленом), если в семействе $L_S(\Psi)$ существует скрученная МП ЛРП порядка m над S .

Ранее скрученные МП ЛРП над полями и кольцами Галуа изучались в [3–26]. Обзор результатов по данной тематике можно найти в [26].

Для проведения некоторых доказательств полезно сформулировать обсуждаемые понятия на матричном языке. Зафиксируем некоторый базис $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ свободного модуля ${}_R S$ и через $a^\downarrow = (a_0, \dots, a_{n-1})^T \in R^{(n)}$ обозначим 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 эндоморфизму $\psi \in \check{S}$ модуля ${}_R S$ соответствует единственная матрица $A(\psi) \in R_{n,n}$, для которой при любом $a \in S$

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

она называется *матрицей эндоморфизма ψ в базисе $\vec{\alpha}$* .

Несложно видеть, что последовательность $v \in S^{(1)}$ является скрученной ЛРП порядка m , т.е. удовлетворяет некоторому соотношению (4), тогда и только тогда, когда столбцы координат $v^\downarrow(i)$ элементов этой последовательности в базисе $\vec{\alpha}$ удовлетворяют соотношению

$$\forall i \in \mathbb{N}_0 \quad v^\downarrow(i+m) = A(\psi_{m-1})v^\downarrow(i+m-1) + \dots + A(\psi_0)v^\downarrow(i). \quad (7)$$

Всюду далее для неотрицательных целых чисел a, b $a \leq b$, через $\overline{a, b}$ мы обозначаем множество $\{a, a+1, \dots, b\}$. Согласно (1) матрицы $A_j = A(\psi_j) \in R_{n \times n}$, $j \in \overline{0, m-1}$, в (7) могут быть произвольными, и закон рекурсии (7) можно записать компактнее:

$$v^\downarrow(i+m) = A_{m-1}v^\downarrow(i+m-1) + \dots + A_0v^\downarrow(i), \quad A_0, \dots, A_{m-1} \in R_{n,n}, \quad i \geq 0. \quad (8)$$

Соотношение (8) будем называть *законом рекурсии скрученной ЛРП v в матричном виде*, а многочлен

$$E_n x^m - A_{m-1} x^{m-1} - \dots - A_1 x - A_0 \in R_{n,n}[x] \quad (9)$$

— *характеристическим многочленом ЛРП v в матричном виде*. В (9) и всюду далее для натурального числа k через E_k обозначаем единичную матрицу размеров $k \times k$ над кольцом R , при этом для $k = n$ полагаем $E = E_n$.

Перед тем как перейти к основным результатам о представлении знаков скрученных МП ЛРП при помощи функции след, напомним основные определения и введем необходимые обозначения. Далее для элемента $s \in S$ обозначим через $\bar{s}$ образ s при действии канонического эпиморфизма $S \rightarrow S/pS$. Рассмотрим p -адическое разрядное множество кольца Галуа S :

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

Оно имеет мощность $q^n = |\bar{S}|$ и удовлетворяет условию $\overline{\Gamma(S)} = \bar{S}$ [2]. При этом каждый элемент $s \in S$ однозначно представляется в виде суммы

$$s = \gamma_0(s) + p\gamma_1(s) + \dots + p^{d-1}\gamma_{d-1}(s), \quad \gamma_0(s), \dots, \gamma_{d-1}(s) \in \Gamma(S), \quad (10)$$

называемой p -адическим разложением элемента s . Далее для целых чисел a, b используем обозначение (a, b) для неотрицательного наибольшего общего делителя a, b . Известно (см., например, [2]), что для каждого такого $j \in \overline{0, n-1}$, что $(n, j) = 1$, отображение $\sigma_j : S \rightarrow S$, задаваемое по правилу

$$\sigma_j(s) = \gamma_0(s)^{q^j} + p\gamma_1(s)^{q^j} + \dots + p^{d-1}\gamma_{d-1}(s)^{q^j},$$

порождает группу $\text{Aut}(S/R)$. При этом традиционно отображение σ_1 называется *автоморфизмом Фробениуса* S над R [2, 27]. Далее будем считать

$$\sigma = \sigma_1.$$

Пусть K — расширение Галуа кольца S степени m . Тогда p -адическое разрядное множество $\Gamma(S)$ есть подполугруппа полугруппы $(\Gamma(K), \cdot)$, каждый элемент $\lambda \in K$ имеет разложение

$$\lambda = \gamma_0(\lambda) + p\gamma_1(\lambda) + \dots + p^{d-1}\gamma_{d-1}(\lambda), \quad \gamma_0(\lambda), \dots, \gamma_{d-1}(\lambda) \in \Gamma(K), \quad (11)$$

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

$$\forall \lambda \in K \quad \varkappa(\lambda) = \gamma_0(\lambda)^q + p\gamma_1(\lambda)^q + \dots + p^{d-1}\gamma_{d-1}(\lambda)^q, \quad (12)$$

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

$$\varkappa|_S = \sigma. \quad (13)$$

Весьма удобным для получения результатов является представление знаков линейных рекуррент с помощью функции след (см., например [2, 28])

$$\mathrm{Tr}_S^K : K \rightarrow S,$$

действующей по правилу

$$\mathrm{Tr}_S^K(\lambda) = \sum_{\eta \in \mathrm{Aut}(K/S)} \eta(\lambda), \quad \lambda \in K.$$

Последнее с учетом (12) для каждого $\lambda \in K$ можно записать в виде

$$\mathrm{Tr}_S^K(\lambda) = \sum_{j=0}^{m-1} \kappa^{nj}(\lambda) = \sum_{j=0}^{m-1} \left(\gamma_0(\lambda)^{q^{nj}} + p\gamma_1(\lambda)^{q^{nj}} + \dots + p^{d-1}\gamma_{d-1}(\lambda)^{q^{nj}} \right). \quad (14)$$

Следуя [2], мы называем унитарный многочлен $G(x) \in S[x]$ многочленом Галуа, если $\bar{G}(x)$ — неприводимый над $\bar{S}$ многочлен. Важнейшую роль в исследовании линейных рекуррентных последовательностей над полями и кольцами Галуа играет следующее утверждение.

Теорема 2 ([2]). Пусть $G(x)$ — многочлен Галуа степени t над S , и ϑ — его корень в K , тогда для любой ЛРП $u \in L_S(G)$ существует единственная константа $\varepsilon \in K$, удовлетворяющая условию

$$u(i) = \mathrm{Tr}_S^K(\varepsilon \vartheta^i), \quad i \geq 0. \quad (15)$$

Поскольку всякий классический МП-многочлен над S есть многочлен Галуа [2], то для знаков классических МП ЛРП имеет место представление (15).

В данной работе изучаются обобщения представления (15) для знаков скрученных МП ЛРП при помощи функции след. При этом можно выделить два направления исследований. К первому относятся исследования, базирующиеся на вложении модуля $L_S(\Psi)$ скрученных МП ЛРП с характеристическим многочленом $\Psi(x) \in \check{S}[x]$ в модуль ЛРП $L_S(F)$ для некоторого многочлена $F(x) \in R[x]$. Такое вложение представляет интерес в связи с тем, что появляется возможность применения математического аппарата, развитого для изучения ЛРП над коммутативными кольцами. Однако при использовании представлений, найденных таким способом, возникают дополнительные условия на элементы колец, участвующих в этих представлениях (см. теорему 4 далее). Учет таких условий подчас весьма затруднителен.

Таким образом, для скрученных МП ЛРП актуальной является задача нахождения представлений, для которых проверка условий на элементы колец, участвующих в представлении, решается относительно просто. Примером такого представления для классических МП ЛРП является (15). Действительно, критерий того, что последовательность (15) является классической МП ЛРП, состоит в том, что порядок элемента ϑ равен τ и элемент ε обратим в K . Отметим, что аналогичное условие для скрученных МП ЛРП имеет более сложный вид (см. теорему 4).

В рамках второго направления исследований получены результаты о представлении скрученных МП ЛРП при помощи функции след из кольца матриц над $\check{S}$ в кольцо $\check{S}$ (см. теорему 8). Основой для получения этих результатов является обобщение теоремы Гамильтона – Кэли, доказанное в [25] и позволяющее для унитарного многочлена над произвольным (вообще говоря, некоммутативным) кольцом с единицей строить расширение кольца, в котором этот многочлен имеет корни. Найденное представление успешно использовано для характеристики МП-многочленов над $\check{S}$ с попарно коммутирующими коэффициентами в законе рекурсии (теорема 11).

Перейдем к результатам первого направления исследований. Заметим, что по предложению 1 для каждой скрученной МП ЛРП v порядка m над S существует такой МП-многочлен $F(x) \in R[x]$ степени mn , что $v \in L_S(F)$. Следовательно, для нахождения некоторого представления скрученной МП ЛРП v в терминах функции след достаточно найти некое представление с помощью функции след рекуррент из $L_S(F)$. Напомним, что $\vec{\alpha} = (\alpha_0, \dots, \alpha_{n-1})$ — базис свободного модуля ${}_R S$.

Теорема 3. Пусть $F(x)$ — МП-многочлен степени mn над R с корнем $\vartheta \in K$. Тогда для любой последовательности $v \in L_S(F)$ существует единственный набор $(b_0, \dots, b_{n-1}) \in K^n$, для которого

$$\forall i \in \mathbb{N}_0 \quad v(i) = \alpha_0 \operatorname{Tr}_R^K(b_0 \vartheta^i) + \alpha_1 \operatorname{Tr}_R^K(b_1 \vartheta^i) + \dots + \alpha_{n-1} \operatorname{Tr}_R^K(b_{n-1} \vartheta^i), \quad (16)$$

и единственный набор $(\varepsilon_0, \dots, \varepsilon_{n-1}) \in K^n$, для которого

$$\forall i \in \mathbb{N}_0 \quad v(i) = \operatorname{Tr}_S^K(\varepsilon_0 \vartheta^i) + \operatorname{Tr}_S^K(\varepsilon_1 \varkappa(\vartheta)^i) + \dots + \operatorname{Tr}_S^K(\varepsilon_{n-1} \varkappa^{n-1}(\vartheta)^i). \quad (17)$$

При этом если $\vec{\beta} = (\beta_0, \dots, \beta_{n-1})$ — базис, двойственный к $\vec{\alpha}$, т.е. справедливо равенство $\operatorname{Tr}_R^S(\alpha_i \beta_j) = e \delta_{ij}$, где δ_{ij} — символ Кронекера,

то для каждого $t \in \overline{0, n-1}$ выполняются условия

$$\varepsilon_t = \sum_{j=0}^{n-1} \alpha_j \kappa^t(b_j), \quad b_t = \sum_{j=0}^{n-1} \sigma^{n-j}(\beta_t) \kappa^{mn-j}(\varepsilon_j) = \sum_{j=0}^{n-1} \kappa^{mn-j}(\beta_t \varepsilon_j). \quad (18)$$

Замечание. Из [29] следует, что для каждого базиса модуля ${}_R S$ существует единственный двойственный базис.

В условиях теоремы 3 будем говорить, что набор $\vec{b} = (b_0, \dots, b_{n-1})$ и набор $\vec{\varepsilon} = (\varepsilon_0, \dots, \varepsilon_{n-1}) \in K^n$ есть *вектор (ϑ) -определяющих коэффициентов ЛРП v (в базисе $\vec{\alpha})$ и определяющий набор (ϑ) -множителей ЛРП v соответственно.*

Представления (16) и (17) можно рассматривать как обобщения представления (15) для скрученных МП ЛРП. Отметим также, что представление (16) впервые было найдено в [3] и здесь приведено для удобства ссылок, а представление (17) было известно лишь для случая, когда $R = \text{GF}(q^d, p^d)$ — поле, т. е. $d = 1$ [22].

Для удобства записи формул для элемента $a \in K$ и произвольного многочлена $a(x) = \sum_{j \geq 0} a_j x^j \in K[x]$ положим

$$a^\varkappa = \varkappa(a), \quad a^\varkappa(x) = \sum_{j \geq 0} \varkappa(a_j) x^j.$$

Пусть $S[x|m]$ — множество многочленов над S степени, меньшей m . Получена следующая характеристика скрученных МП ЛРП порядка m в классе последовательностей из $L_S(F)$ в терминах определяющих наборов множителей.

Теорема 4. Пусть $F(x)$ — МП-многочлен над R степени mn с корнем $\vartheta \in K$ и $v \in L_S(F)$ — последовательность из семейства $L_S(F)$ с определяющим набором ϑ -множителей $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1})$, т. е. выполнено равенство (17). Положим $\xi = \varkappa^{n-1}(\vartheta)$. Последовательность v есть скрученная МП ЛРП порядка m над S тогда и только тогда, когда выполнено условие

$$\forall c(x) \in S[x|m] \setminus \{0\} : \quad \varepsilon_{n-1} c(\xi) + \varepsilon_{n-2}^\varkappa c^\sigma(\xi) + \dots + \varepsilon_0^{\varkappa^{n-1}} c^{\sigma^{n-1}}(\xi) \neq 0. \quad (19)$$

Задачу проверки условия (19) можно существенно упростить. Зафиксируем некоторые базисы $\vec{\lambda} = (\lambda_0, \dots, \lambda_{mn-1})$ и $\vec{\mu} = (\mu_0, \dots, \mu_{m-1})$ свободных модулей ${}_R K$ и ${}_S K$ соответственно. Пусть столбец координат $(\lambda_j)_{\vec{\mu}}^\downarrow$ элемента λ_j в базисе $\vec{\mu}$ имеет вид $(\lambda_j)_{\vec{\mu}}^\downarrow = (\lambda_{j0}, \dots, \lambda_{j,m-1})^T$.

Для последовательности v с определяющим набором ϑ -множителей $(\varepsilon_0, \dots, \varepsilon_{n-1})$ положим

$$D_j = ((\varepsilon_j^{\mathcal{K}^{n-1-j}})_{\vec{\mu}}^\downarrow, (\varepsilon_j^{\mathcal{K}^{n-1-j}} \xi)_{\vec{\mu}}^\downarrow, \dots, (\varepsilon_j^{\mathcal{K}^{n-1-j}} \xi^{m-1})_{\vec{\mu}}^\downarrow) \in S_{m \times m}, \quad j \in \overline{0, n-1}. \quad (20)$$

Предложение 5. Условие (19) выполнено тогда и только тогда, когда обратима матрица $B \in R_{mn \times mn}$, столбцы которой имеют вид

$$(B_j)^\downarrow = \left(\vec{\mu} \left(D_{n-1} \begin{pmatrix} \lambda_{j0} \\ \lambda_{j1} \\ \vdots \\ \lambda_{j,m-1} \end{pmatrix} + D_{n-2} \begin{pmatrix} \lambda_{j0}^{\mathcal{K}} \\ \lambda_{j1}^{\mathcal{K}} \\ \vdots \\ \lambda_{j,m-1}^{\mathcal{K}} \end{pmatrix} + \dots + D_0 \begin{pmatrix} \lambda_{j0}^{\mathcal{K}^{n-1}} \\ \lambda_{j1}^{\mathcal{K}^{n-1}} \\ \vdots \\ \lambda_{j,m-1}^{\mathcal{K}^{n-1}} \end{pmatrix} \right) \right)_{\vec{\lambda}}^\downarrow,$$

где $j \in \overline{0, mn-1}$.

Отметим, что основной результат о представлении классических МП ЛРП над кольцами Галуа при помощи функции след (теорема 2) базируется на том наблюдении, что произвольный унитарный многочлен $G(x) \in S[x]$ имеет корень в фактор-кольце $S[x]/S[x]G(x)$. Оно же позволяет получить представления для знаков скрученных МП ЛРП при помощи функции след из теоремы 3. Однако заметим, что данный указанный корень может не существовать в случае многочленов над некоммутативными кольцами, в частности для многочленов $\Psi(x) \in \check{S}[x]$. Это связано с тем, что множество $\check{S}[x]/\check{S}[x]\Psi(x)$ не имеет структуры кольца, так как идеал $\check{S}[x]\Psi(x)$ является, вообще говоря, односторонним идеалом, а не двусторонним [31]. В [25] для произвольного унитарного многочлена $A(x)$ над кольцом с единицей (возможно, некоммутативным) построено расширение кольца, содержащее корни этого многочлена. Там же для МП-многочленов над $\check{S}$ исследована структура их корней в таком расширении.

Приведем необходимые для дальнейшего изложения результаты из [25]. Далее $\mathcal{K} = \check{S}_{m,m}$. Для произвольного элемента $\psi \in \check{S}$ будем использовать обозначение $D(\psi) = \text{diag}(\psi, \dots, \psi) \in \mathcal{K}$. Для упрощения обозначений без ограничения общности можно считать, что $\check{S} \subset \mathcal{K}$, за счет отождествления элементов $\psi \in \check{S}$ и $D(\psi) \in \mathcal{K}$. Для произвольного многочлена

$$H(x) = \sum_{j \geq 0} h_j x^j \in \check{S}[x]$$

и элемента $\beta \in \mathcal{K}$ положим

$$H(\beta) = \sum_{j \geq 0} D(h_j) \beta^j \in \mathcal{K}. \quad (21)$$

Если $H(\beta) = 0$, то β будем называть *корнем* $H(x)$ в $\mathcal{K}$.

Обозначим через $RT_{\mathcal{K}}(H)$ множество корней в $\mathcal{K}$ многочлена $H(x) \in \check{S}[x]$. Далее, $\mathcal{K}^*$ — мультипликативная группа кольца $\mathcal{K}$. Для порядка произвольного элемента γ в группе K^* мы используем стандартное обозначение $\text{ord } \gamma$. Следующее утверждение обосновывает существование корней в $\mathcal{K}$ унитарных многочленов над $\check{S}$ и описывает некоторые свойства множества корней МП-многочленов над $\check{S}$.

Теорема 6 ([25]). Пусть $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$ — многочлен над $\check{S}$. Тогда $RT_{\mathcal{K}}(\Psi) \neq \emptyset$. Более того, в случае когда $\Psi(x)$ есть МП-многочлен, справедливы следующие утверждения.

- 1) Мощность $|RT_{\mathcal{K}}(\Psi)|$ множества $RT_{\mathcal{K}}(\Psi)$ делится на m .
- 2) Если $\gamma \in RT_{\mathcal{K}}(\Psi)$, то $\gamma \in \mathcal{K}^*$ и $\text{ord } \gamma = \tau$.
- 3) Если $\gamma \in RT_{\mathcal{K}}(\Psi)$, то для любого ненулевого многочлена $H(x)$ над $\check{S}$ степени, меньшей m , выполняется условие $H(\gamma) \neq 0$.
- 4) Все корни $\Psi(x)$ в $\mathcal{K}$ сопряжены по модулю p , т.е.

$$\forall \beta, \gamma \in RT_{\mathcal{K}}(\Psi) \exists \mu \in \mathcal{K}^* : \gamma - \mu^{-1} \beta \mu \in p\mathcal{K}.$$

- 5) $\Psi(x)$ не имеет кратных корней в $\mathcal{K}$.

Отметим, что доказательство теоремы 6 опирается на полученное в [25] обобщение теоремы Гамильтона–Кэли (см., например, [32, 33]) на специальный класс матриц над некоммутативными кольцами с единицей. Для удобства приведем точную формулировку.

Пусть Q — произвольное (не обязательно коммутативное) кольцо с единицей. Будем говорить, что матрица $A \in Q_{m,m}$ обладает свойством $(*)$, если

$$\forall i_1, i_2, j_1, j_2 \in \overline{1, m}, j_1 \neq j_2 : a_{i_1 j_1} a_{i_2 j_2} = a_{i_2 j_2} a_{i_1 j_1}, \quad (*)$$

и обладает свойством $(**)$, если

$$\forall i_1, i_2, j_1, j_2 \in \overline{1, m}, i_1 \neq i_2 : a_{i_1 j_1} a_{i_2 j_2} = a_{i_2 j_2} a_{i_1 j_1}. \quad (**)$$

Далее, пусть $\mathbf{P}(\overline{1, m})$ — множество перестановок множества $\overline{1, m} = \{1, 2, \dots, m\}$. Для перестановки $(i_1, \dots, i_m) \in \mathbf{P}(\overline{1, m})$ обозначим через $\delta(i_1, \dots, i_m)$ ее *четность* [32]. По аналогии со случаем матриц над коммутативным кольцом для матрицы $A \in Q_{m,m}$ рассмотрим ее *определитель*, вычисляемый по формуле

$$\sum_{(i_1, \dots, i_m) \in \mathbf{P}(\overline{1, m})} \delta(i_1, \dots, i_m) \prod_{j=1}^m a_{ji_j}. \quad (22)$$

Отметим, что в силу некоммутативности кольца Q значение суммы (22), вообще говоря, может зависеть от порядка вычисления произведений. Будем говорить, что определитель матрицы $A \in Q_{m,m}$ *определен корректно*, если значение суммы (22) не зависит от порядка сомножителей в произведениях, при этом значение суммы (22) будем обозначать $\text{Det}(A)$. В частности, для матриц A , обладающих свойством (*) или (**), определитель определен корректно. Множество матриц из $Q_{m,m}$, обладающих свойством (*) или (**), обозначим через

$$WD_m(Q).$$

Следующий результат является обобщением теоремы Гамильтона – Кэли.

Теорема 7 ([25]). Пусть $A \in WD_m(Q)$. Тогда $Ex - A \in WD_m(Q[x])$, и если $H(x) = \text{Det}(Ex - A)$, то

- 1) $H(A^T) = 0$, если A обладает свойством (*),
- 2) $H(A) = 0$, если A обладает свойством (**).

Напомним, что $R = \text{GR}(q^d, p^d)$, S — расширение Галуа степени n кольца R , $\check{S}$ — кольцо эндоморфизмов S над R и что внешнее умножение элемента $\psi \in \check{S}$ на элемент $s \in S$ задается формулой $\psi \circ s = \psi(s)$ (см. (2)). При таком определении кольцо S есть левый $\check{S}$ -модуль.

Определим функцию

$$\text{Tr}_{\check{S}}^{\mathcal{K}} : \mathcal{K} \rightarrow \check{S},$$

действующую на элементе $A = (\psi_{ij})_{i,j=1}^m \in \mathcal{K}$, формулой

$$\text{Tr}_{\check{S}}^{\mathcal{K}}(A) = \psi_{11} + \psi_{22} + \dots + \psi_{mm}. \quad (23)$$

Несложно видеть, что $\text{Tr}_{\check{S}}^{\mathcal{K}}$ есть эпиморфизм модулей ${}_S\mathcal{K}$ и ${}_S\check{S}$.

Далее в этом разделе R — поле, т. е. $d = 1$. Теорема 6 и теорема 7 позволяют получить новое представление при помощи функции след (23) для знаков скрученных МП ЛРП, в некотором смысле более близкое к представлению (15), нежели представления в теореме 3. Для произвольного элемента $\gamma \in \mathcal{K}$ через $R[\gamma]$ мы обозначаем подкольцо в $\mathcal{K}$, порожденное γ над R , т. е. наименьшее по включению подкольцо кольца $\mathcal{K}$, содержащее γ и R . Основой для приводимых далее результатов служит следующая теорема.

Теорема 8. Пусть $v \in L_S(\Psi)$ — скрученная МП ЛРП порядка t с характеристическим многочленом $\Psi(x)$. Тогда для любого элемента $\gamma \in RT_{\mathcal{K}}(\Psi)$ найдутся такие элемент $\varepsilon \in R[\gamma]$ и элемент $s \in S$, что

$$\forall i \in \mathbb{N}_0 \quad v(i) = \text{Tr}_{\mathcal{K}}^{\mathcal{K}}(\gamma^i \varepsilon) \circ s. \quad (24)$$

Представление (24) в некоторых случаях оказывается удобнее представлений (16) и (17). В частности, иногда оно позволяет изучать регулярные выборки (см., например, [32]) из скрученных МП ЛРП.

Следствие 9. Пусть $v \in L_S(\Psi)$ — скрученная МП ЛРП порядка t и для всех $i \geq 0$ справедливо равенство $v(i) = \text{Tr}_{\mathcal{K}}^{\mathcal{K}}(\gamma^i \varepsilon) \circ s$ при некоторых $\gamma \in RT_{\mathcal{K}}(\Psi)$, $\varepsilon \in \mathcal{K}$, $s \in S$. Тогда если матрица γ^t обладает свойством $(**)$ при некотором числе $t \in \mathbb{N}$, $(t, \tau) = 1$, то последовательность

$$w(i) = v(ti) = \text{Tr}_{\mathcal{K}}^{\mathcal{K}}(\gamma^{ti} \varepsilon) \circ s, \quad i \in \mathbb{N}_0, \quad (25)$$

есть скрученная МП ЛРП порядка t с характеристическим многочленом

$$\text{Det}(Ex - \gamma^t). \quad (26)$$

В частности, если все коэффициенты многочлена $\Psi(x)$ попарно коммутируют, то для любого $t \in \mathbb{N}$, $(t, \tau) = 1$, последовательность (25) есть скрученная МП ЛРП порядка t с характеристическим многочленом (26).

Первым существенным применением теоремы 8 является характеристизация МП-многочленов над $\check{S}$ с попарно коммутирующими коэффициентами. Прежде чем перейти к формулировке данного результата, введем необходимые понятия и обоснуем актуальность задачи описания таких многочленов с точки зрения криптографии.

Напомним, что через $\check{S}^*$ мы обозначаем мультипликативную группу кольца $\check{S}$. Следующая теорема дает первый конструктивный способ

построения целого класса скрученных МП ЛРП из одной скрученной МП ЛРП над кольцом Галуа.

Теорема 10 ([3]). Пусть v — скрученная МП ЛРП порядка t над S с характеристическим многочленом $\Psi(x) = x^m - \sum_{i=0}^{m-1} \psi_i x^i \in \check{S}[x]$, $\psi \in \check{S}$, и $w = \psi(v)$ — последовательность элементов $w(i) = \psi(v(i))$, $i \in \mathbb{N}_0$. Тогда:

- 1) если $\psi \in \check{S}^*$, то w есть скрученная МП ЛРП с характеристическим многочленом $\Psi'(x) = x^m - \sum_{i=0}^{m-1} (\psi \cdot \psi_i \cdot \psi^{-1}) x^i$,
- 2) если w есть скрученная МП ЛРП порядка t над S , то $\psi \in \check{S}^*$.

Если v — классическая МП ЛРП порядка t над кольцом S (т. е. если $\Psi(x) \in S[x]$), то будем называть скрученную МП ЛРП $w = \psi(v)$ и соответствующий МП-многочлен $\Psi'(x)$ *линеаризуемыми*. Перебирая все $\psi \in \check{S}^*$, можно из одного классического МП-многочлена $\Psi(x)$ получить по формуле из п. 1 довольно большую серию МП-многочленов над $\check{S}$ [3]. Класс линеаризуемых МП-многочленов полностью описан в [3]. Там же точно вычислена его мощность. Отметим, что все коэффициенты линеаризуемого МП-многочлена попарно коммутируют.

Далее через $\text{rank}_S v$, $\text{rank}_R v$ обозначим ранг (степень минимального многочлена) последовательности $v \in S^{(1)}$, рассматриваемой как ЛРП над модулями ${}_S S$ и ${}_R S$ соответственно (см. [1]).

Из [3] следует, что для любой скрученной МП ЛРП v над кольцом S выполняется равенство $\text{rank}_R v = mn$. Если v — классическая МП ЛРП над кольцом S , то $\text{rank}_S v = m$. В случае когда v — скрученная МП ЛРП над S , справедливы неравенства

$$m \leq \text{rank}_S v \leq nm. \quad (27)$$

Одним из обстоятельств, вызывающих интерес к скрученным МП ЛРП, является то, что для них левое неравенство в (27) является строгим всегда, за исключением «тривиального» случая, когда v — классическая МП ЛРП над модулем ${}_S S$. Кроме того, в [22, 23] указаны способы построения скрученных МП ЛРП v порядка t , для которых правое неравенство в (27) достижимо. Заметим также, что в [8–10] показано, что наилучшими с точки зрения криптографии алгебраическими характеристиками обладают усложнения скрученных МП ЛРП, имеющих максимальный ранг.

Известно (см., например, [3]), что если v — скрученная МП ЛРП порядка t над S и $\psi \in \check{S}^*$, то ранг $\text{rank}_S \psi(v)$ последовательности

$w = \psi(v)$ может быть как больше значения $\text{rank}_S(v)$, так и меньше. В частности, для любой линейризуемой МП ЛРП v порядка m над S существует такой элемент $\psi \in \check{S}$, что $\text{rank}_S v = m$. Таким образом, одним из критериев выбора МП-многочлена $\Psi(x) \in \check{S}[x]$ степени m является требование, чтобы для любой скрученной МП ЛРП $v \in L_S(\Psi)$ и любого элемента $\psi \in \check{S}^*$ выполнялось условие $\text{rank}_S \psi(v) = mn$, т. е.

$$\forall v \in L_S(\Psi) \setminus \{0\}, \forall \psi \in \check{S}^* : \text{rank}_S \psi(v) = mn. \quad (28)$$

Примеры МП-многочленов, обладающих свойством (28), построены в [7].

Не менее важным требованием, предъявляемым к МП-многочленам, является удобство реализации операций умножения на их коэффициенты и возможность хранения в памяти данных коэффициентов в наиболее экономном виде. Одним из классов МП-многочленов над $\check{S}$, удовлетворяющих этому требованию, является класс МП-многочленов вида

$$\Psi(x) = x^m - \xi \cdot (r_{m-1}x^{m-1} + \dots + r_1x + r_0) = x^m - r_{m-1}\xi x^{m-1} - \dots - r_1\xi x - r_0\xi, \quad (29)$$

где $\xi \in \check{S}, r_0, \dots, r_{m-1} \in R$. Заметим, что для хранения такого многочлена достаточно хранить элемент $\xi \in \check{S}$ и набор констант $r_0, \dots, r_{m-1} \in R$. При хранении же МП-многочлена произвольного вида над $\check{S}$ степени m может потребоваться хранить m элементов кольца $\check{S}$. МП-многочлены вида (29) впервые исследовались в [12] и рассматривались как перспективный источник законов рекурсии для векторных регистров сдвига, используемых для построения поточных шифрсистем. В дальнейшем МП-многочлены (29) изучались в [17, 18]. Отметим, что коэффициенты многочленов (29) так же, как и коэффициенты линейризуемых МП-многочленов, попарно коммутируют. Таким образом, задача описания МП-многочленов над $\check{S}$ с попарно коммутирующими коэффициентами в законе рекурсии представляет интерес для криптографии в связи с синтезом поточных шифрсистем.

Следующая теорема описывает скрученные МП ЛРП порядка m над полем, у которых коэффициенты в характеристическом многочлене степени m попарно коммутируют.

Теорема 11. Пусть $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$ — МП-многочлен со свойством

$$\psi_k \psi_l = \psi_l \psi_k. \quad (30)$$

Тогда $\Psi(x)$ — линейризуемый МП-многочлен.

Теорема 11 показывает, что МП-многочлены над $\check{S}$ вида (29) не удовлетворяют критерию (28).

2. Доказательства

2.1. Доказательство теоремы 3

Если $\vec{\alpha}$ — базис свободного модуля ${}_R S$, то любой последовательности $v \in S^{(1)}$ соответствует единственный набор последовательностей $v_0, \dots, v_{n-1} \in R^{(1)}$, удовлетворяющих равенству

$$v = v_0\alpha_0 + v_1\alpha_1 + \dots + v_{n-1}\alpha_{n-1}. \quad (31)$$

Будем называть $v_0, \dots, v_{n-1}$ *координатными последовательностями* последовательности v (в базисе $\vec{\alpha}$). Отметим, что ранее в отечественной литературе (см., например, [2, 30]) термин «координатные последовательности» использовался для последовательностей другого типа, которые в настоящее время называются разрядными последовательностями (см., например, [8, 9]). Далее нам понадобится следующее утверждение.

Теорема 12 ([3]). *Последовательность $v \in S^{(1)}$ является скрученной МП ЛРП порядка m тогда и только тогда, когда*

$$\forall i \in \mathbb{N}_0 : v[\overline{i, i+m-1}] \notin (pS)^m, \quad (32)$$

и существует такой МП-многочлен $F(x) \in R[x]$ степени mn , что выполняется условие $v \in L_S(F)$.

Любая скрученная МП ЛРП v является реверсивной (чисто периодической), и при выполнении условия $v \in L_S(F)$ система координатных последовательностей из ее разложения (31) есть линейно независимая система МП ЛРП из $L_R(F)$.

По теореме 12 все координатные последовательности $v_0, \dots, v_{n-1}$ линейной рекурренты $v \in L_S(F)$ принадлежат семейству $L_R(F)$. Теперь для доказательства (16) осталось воспользоваться теоремой 2.

Перейдем к доказательству (17). Продолжим отображение $\varkappa: K \rightarrow K$ на кольцо $K[x]$ естественным образом по правилу

$$\varkappa\left(\sum_{j \geq 0} a_j x^j\right) = \sum_{j \geq 0} \varkappa(a_j) x^j. \quad (33)$$

Несложно проверить, что при таком определении отображение $\varkappa$ есть автоморфизм кольца $K[x]$. В дальнейшем в случае, когда K — поле, а автоморфизм $\varkappa$ есть возведение в степень q , для многочлена $A(x) \in K[x]$ будем писать

$$A^{(q)}(x) = \varkappa(A(x)).$$

Напомним, что многочлены $A(x), B(x) \in K[x]$ называются взаимно простыми, если существуют такие многочлены $C(x), D(x) \in K[x]$, что

$$C(x)A(x) + D(x)B(x) = e.$$

Лемма 13. *Многочлен $F(x)$ из теоремы 3 может быть представлен в виде*

$$F(x) = G(x)\varkappa(G(x)) \dots \varkappa^{n-1}(G(x)), \quad (34)$$

где $G(x), \varkappa(G(x)), \dots, \varkappa^{n-1}(G(x)) \in S[x]$ суть попарно взаимно простые МП-многочлены степени m .

Доказательство леммы 13. Согласно [2] многочлен $F(x)$ имеет следующее разложение над K

$$F(x) = \prod_{j=0}^{mn-1} (x - \varkappa^j(\vartheta)), \quad (35)$$

при этом $\text{ord } \vartheta = (q^{mn} - 1)p^{d-1}$. Также из [2] известно

$$S[x] = \{H(x) \in K[x] : \varkappa^n(H(x)) = H(x)\}. \quad (36)$$

Рассмотрим многочлен

$$G(x) = \prod_{j=0}^{m-1} (x - \varkappa^{nj}(\vartheta)) \in K[x]$$

и положим $G_l(x) = \varkappa^l(G(x))$ для $l \in \mathbb{N}_0$. В силу того что $\varkappa$ — автоморфизм кольца $K[x]$, имеем $\varkappa^n(G(x)) = G(x)$, следовательно, согласно (36) выполняется условие $G(x) \in S[x]$.

Из условия (35) нетрудно вывести, что $\varkappa^l(G(x)) | F(x)$ для всех значений $l \in \overline{0, n-1}$.

Лемма 14. *Многочлены $G_0(x), \dots, G_{n-1}(x)$ попарно взаимно просты.*

Доказательство леммы 14. Справедливы равенства

$$G_l(x) = \varkappa^l(G(x)) = \varkappa^l \left(\prod_{t \in \overline{0, m-1}} (x - \varkappa^{nt}(\vartheta)) \right) = \prod_{t \in \overline{0, m-1}} (x - \varkappa^{nt}(\varkappa^l(\vartheta))). \quad (37)$$

Напомним, что через $\bar{a}$ мы обозначаем образ элемента $a \in K$ при каноническом эпиморфизме $\rho : K \rightarrow K/pK$. Известно (см., например, [2]), что произвольный элемент $a \in K$ обратим в K тогда и только тогда, когда обратим его образ $\bar{a}$. Для доказательства леммы 14 достаточно заметить, что если $t, t' \in \overline{0, m-1}$, $l, l' \in \overline{0, n-1}$ и упорядоченные наборы (t, l) , (t', l') различны, то разность элементов $\varkappa^{nt}(\varkappa^l(\vartheta)) = \varkappa^{nt+l}(\vartheta)$ и $\varkappa^{nt'}(\varkappa^{l'}(\vartheta)) = \varkappa^{nt'+l'}(\vartheta)$ есть обратимый элемент кольца K , поскольку $\bar{\vartheta}$ — примитивный элемент поля $\bar{K}$. Следовательно, многочлены $x - \varkappa^{nt}(\varkappa^l(\vartheta))$ и $x - \varkappa^{nt'}(\varkappa^{l'}(\vartheta))$ взаимно просты. Отсюда и из (37) следует, что если $l \neq l'$, $l, l' \in \overline{0, n-1}$, то многочлены $G_l(x)$ и $G_{l'}(x)$ взаимно просты. Лемма 14 доказана. $\square$

Вернемся к доказательству леммы 13. По лемме 14 многочлен

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

делит многочлен $F(x)$. Для завершения доказательства осталось заметить, что $H(x)$ — унитарный и его степень равна степени $F(x)$. Лемма 13 доказана. $\square$

Вернемся к доказательству теоремы 3. Так как сомножители в разложении (34) попарно взаимно просты, то имеет место разложение

$$L_S(F) = L_S(G_0) \dot{+} \dots \dot{+} L_S(G_{n-1}), \quad (38)$$

ввиду которого последовательность v однозначно представляется в виде суммы

$$v = v^{(0)} + \dots + v^{(n-1)}, \quad v^{(t)} \in L_S(G_t), \quad t \in \overline{0, n-1}. \quad (39)$$

В силу (37) для каждой последовательности $v^{(l)}$ в (39) существует единственный элемент $\varepsilon_l \in K$, при котором

$$\forall i \in \mathbb{N}_0 \quad v^{(l)}(i) = \text{Tr}_S^K(\varepsilon_l \varkappa^l(\vartheta)^i), \quad (40)$$

где $l \in \overline{0, n-1}$. Теперь (17) следует из соотношений (38)–(40).

Докажем первое равенство в (18). Из (16) имеем

$$v(i) = \sum_{j=0}^{n-1} \alpha_j \operatorname{Tr}_R^K(b_j \vartheta^i) = \sum_{j=0}^{n-1} \alpha_j \sum_{l=0}^{mn-1} \varkappa^l(b_j \vartheta^i) = \sum_{j=0}^{n-1} \alpha_j \sum_{k=0}^{m-1} \sum_{t=0}^{n-1} \varkappa^{kn+t}(b_j \vartheta^i). \quad (41)$$

Так как $\varkappa$ — автоморфизм, то из (41) находим

$$v(i) = \sum_{j=0}^{n-1} \alpha_j \sum_{t=0}^{n-1} \varkappa^t \left(\sum_{k=0}^{m-1} \varkappa^{kn}(b_j \vartheta^i) \right) = \sum_{j=0}^{n-1} \alpha_j \sum_{t=0}^{n-1} \varkappa^t (\operatorname{Tr}_S^K(b_j \vartheta^i)).$$

Отсюда и из условия $\alpha_j \in S$ получаем

$$v(i) = \operatorname{Tr}_S^K \left(\sum_{t=0}^{n-1} \varkappa^t(\vartheta^i) \sum_{j=0}^{n-1} \alpha_j \varkappa^t(b_j) \right). \quad (42)$$

Теперь первое равенство в (18) следует из единственности определяющего набора ϑ -множителей ЛРП v .

Докажем второе равенство в (18). Применяя автоморфизм κ^{mn-t} к обеим частям равенства $\varepsilon_t = \sum_{j=0}^{n-1} \alpha_j \kappa^t(b_j)$ для каждого $t \in \overline{0, n-1}$, с учетом (13) находим

$$\kappa^{mn-t}(\varepsilon_t) = \sum_{j=0}^{n-1} \kappa^{mn-t}(\alpha_j) b_j = \sum_{j=0}^{n-1} \sigma^{n-t}(\alpha_j) b_j.$$

Последнее равносильно условию

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \\ \sigma^{n-1}(\alpha_0) & \sigma^{n-1}(\alpha_1) & \dots & \sigma^{n-1}(\alpha_{n-1}) \\ \dots & \dots & \dots & \dots \\ \sigma(\alpha_0) & \sigma(\alpha_1) & \dots & \sigma(\alpha_{n-1}) \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} \varepsilon_0 \\ \kappa^{mn-1}(\varepsilon_1) \\ \vdots \\ \kappa^{mn-n+1}(\varepsilon_{n-1}) \end{pmatrix}.$$

В силу двойственности базисов $\vec{\alpha}$ и $\vec{\beta}$ произведение

$$\begin{pmatrix} \beta_0 & \sigma^{n-1}(\beta_0) & \dots & \sigma(\beta_0) \\ \beta_1 & \sigma^{n-1}(\beta_1) & \dots & \sigma(\beta_1) \\ \dots & \dots & \dots & \dots \\ \beta_{n-1} & \sigma^{n-1}(\beta_{n-1}) & \dots & \sigma(\beta_{n-1}) \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \\ \sigma^{n-1}(\alpha_0) & \sigma^{n-1}(\alpha_1) & \dots & \sigma^{n-1}(\alpha_{n-1}) \\ \dots & \dots & \dots & \dots \\ \sigma(\alpha_0) & \sigma(\alpha_1) & \dots & \sigma(\alpha_{n-1}) \end{pmatrix}$$

равно единичной матрице E размера $n \times n$. Таким образом, справедливо равенство

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} \beta_0 & \sigma^{n-1}(\beta_0) & \dots & \sigma(\beta_0) \\ \beta_1 & \sigma^{n-1}(\beta_1) & \dots & \sigma(\beta_1) \\ \dots & \dots & \dots & \dots \\ \beta_{n-1} & \sigma^{n-1}(\beta_{n-1}) & \dots & \sigma(\beta_{n-1}) \end{pmatrix} \cdot \begin{pmatrix} \varepsilon_0 \\ \kappa^{mn-1}(\varepsilon_1) \\ \vdots \\ \kappa^{mn-n+1}(\varepsilon_{n-1}) \end{pmatrix},$$

из которого следует справедливость второго равенства в (18). Теорема 3 доказана.

2.2. Доказательство теоремы 4

Пусть $\vec{\alpha} = (\alpha_0, \dots, \alpha_{n-1})$, $\vec{\beta} = (\beta_0, \dots, \beta_{n-1})$ — пара двойственных базисов модуля ${}_R S$, т.е. для любых $i, j \in \overline{0, n-1}$ выполняется равенство $\text{Tr}_R^S(\alpha_i \beta_j) = e \delta_{ij}$, где δ_{ij} — символ Кронекера. Напомним, что согласно [29] для каждого базиса модуля ${}_R S$ существует единственный двойственный к нему базис. Рассмотрим вектор $(b_0, \dots, b_{n-1}) \in K^n$ ϑ -определяющих коэффициентов ЛРП v в базисе $\vec{\alpha}$. С учетом соотношений (18) для каждого $t \in \overline{0, n-1}$ имеем

$$b_t = \sum_{j=0}^{n-1} \varepsilon_j^{\kappa^{mn-j}} \beta_t^{\sigma^{n-j}}. \quad (43)$$

Согласно [3] последовательность v есть скрученная МП ЛРП тогда и только тогда, когда система

$$\vec{\theta} = (b_0, \dots, b_{n-1}, b_0 \vartheta, \dots, b_{n-1} \vartheta, \dots, \dots, b_0 \vartheta^{m-1}, \dots, b_{n-1} \vartheta^{m-1}) \quad (44)$$

есть базис свободного модуля ${}_R K$. Последнее выполнено тогда и только тогда, когда для любого ненулевого набора $(a_0, \dots, a_{mn-1}) \in R^{mn}$ имеет место неравенство

$$\sum_{t=0}^{n-1} a_t b_t + \vartheta \sum_{t=n}^{2n-1} a_t b_{t-n} + \dots + \vartheta^{m-1} \sum_{t=m(n-1)}^{mn-1} a_t b_{t-(m-1)n} \neq 0. \quad (45)$$

Подставляя выражение для b_t из (43) в (45), находим, что условие (45) равносильно условию

$$\begin{aligned} \sum_{t=0}^{n-1} a_t \sum_{j=0}^{n-1} \varepsilon_j^{\kappa^{mn-j}} \beta_t^{\sigma^{n-j}} + \vartheta \sum_{t=n}^{2n-1} a_t \sum_{j=0}^{n-1} \varepsilon_j^{\kappa^{mn-j}} \beta_{t-n}^{\sigma^{n-j}} + \dots \\ + \vartheta^{m-1} \sum_{t=m(n-1)}^{mn-1} a_t \sum_{j=0}^{n-1} \varepsilon_j^{\kappa^{mn-j}} \beta_{t-(m-1)n}^{\sigma^{n-j}} \neq 0. \end{aligned} \quad (46)$$

Последнее выполнено, если и только если

$$\begin{aligned} \sum_{j=0}^{n-1} \varepsilon_j^{\varkappa^{mn-j}} \sum_{t=0}^{n-1} a_t \beta_t^{\sigma^{n-j}} + \sum_{j=0}^{n-1} \varepsilon_j^{\varkappa^{mn-j}} \vartheta \sum_{t=n}^{2n-1} a_t \beta_{t-n}^{\sigma^{n-j}} + \dots \\ + \sum_{j=0}^{n-1} \varepsilon_j^{\varkappa^{mn-j}} \vartheta^{m-1} \sum_{t=m(n-1)}^{mn-1} a_t \beta_{t-(m-1)n}^{\sigma^{n-j}} \neq 0. \end{aligned} \quad (47)$$

Далее, из (13) следует, что для любых $t, j \in \overline{0, n-1}$ выполняются равенства

$$\beta_t^{\sigma^{n-j}} = \beta_t^{\varkappa^{mn-j}}. \quad (48)$$

Тогда, поскольку $a_t \in R$, выполняются равенства $a_t^{\varkappa^{mn-j}} = a_t$ для всех $j \in \overline{0, mn-1}$. Следовательно, (47) равносильно условию

$$\begin{aligned} \sum_{j=0}^{n-1} \varepsilon_j^{\varkappa^{mn-j}} \left(\sum_{t=0}^{n-1} a_t^{\varkappa^{mn-j}} \beta_t^{\varkappa^{mn-j}} + (\vartheta^{\varkappa^j})^{\varkappa^{mn-j}} \sum_{t=n}^{2n-1} a_t^{\varkappa^{mn-j}} \beta_{t-n}^{\varkappa^{mn-j}} + \dots \right. \\ \left. + \left((\vartheta^{m-1})^{\varkappa^j} \right)^{\varkappa^{mn-j}} \sum_{t=m(n-1)}^{mn-1} a_t^{\varkappa^{mn-j}} \beta_{t-(m-1)n}^{\varkappa^{mn-j}} \right) \neq 0. \end{aligned} \quad (49)$$

Пользуясь тем, что $\varkappa$ — автоморфизм кольца K , преобразуем левую часть (49) к виду

$$\sum_{j=0}^{n-1} \left(\varepsilon_j \left(\sum_{t=0}^{n-1} a_t \beta_t + \vartheta^{\varkappa^j} \sum_{t=n}^{2n-1} a_t \beta_{t-n} + \dots + (\vartheta^{m-1})^{\varkappa^j} \sum_{t=m(n-1)}^{mn-1} a_t \beta_{t-(m-1)n} \right) \right)^{\varkappa^{mn-j}}.$$

Поскольку система $\vec{\beta}$ — базис модуля ${}_R S$, неравенство (49) выполнено тогда и только тогда, когда для любого многочлена $c(x) \in S[x|m] \setminus \{0\}$ имеет место неравенство

$$\sum_{j=0}^{n-1} \kappa^{mn-j} (\varepsilon_j c(\vartheta^{\varkappa^j})) \neq 0. \quad (50)$$

Применяя автоморфизм $\varkappa^{n-1}$ к обеим частям соотношения (50), находим, что v есть скрученная МП ЛРП порядка m над кольцом S , если и только если для любого многочлена $c(x) \in S[x|m] \setminus \{0\}$ выполняется условие

$$\sum_{j=0}^{n-1} \kappa^{n-1-j} (\varepsilon_j c(\vartheta^{\varkappa^j})) = \sum_{j=0}^{n-1} \varepsilon^{\kappa^{n-1-j}} c^{\sigma^{n-1-j}} (\vartheta^{\varkappa^{n-1}}) \neq 0.$$

Теорема доказана.

2.3. Доказательство предложения 5

Несложно видеть, что для фиксированного многочлена $c(x) \in S[x|m] \setminus \{0\}$ условие (19) можно записать в виде

$$(\varepsilon_{n-1}, \varepsilon_{n-1}\xi, \dots, \varepsilon_{n-1}\xi^{m-1}, \dots, \varepsilon_0^{\varkappa^{n-1}}, \varepsilon_0^{\varkappa^{n-1}}\xi, \dots, \varepsilon_0^{\varkappa^{n-1}}\xi^{m-1}) \cdot (c_0, c_1, \dots, c_{m-1}, \dots, c_0^{\varkappa^{n-1}}, c_1^{\varkappa^{n-1}}, \dots, c_{m-1}^{\varkappa^{n-1}})^T \neq 0. \quad (51)$$

Напомним, что матрицы $D_j, j \in \overline{0, n-1}$, определены в (20). Условие (51) равносильно условию

$$D_{n-1} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} + D_{n-2} \begin{pmatrix} c_0^{\varkappa} \\ c_1^{\varkappa} \\ \vdots \\ c_{m-1}^{\varkappa} \end{pmatrix} + \dots + D_0 \begin{pmatrix} c_0^{\varkappa^{n-1}} \\ c_1^{\varkappa^{n-1}} \\ \vdots \\ c_{m-1}^{\varkappa^{n-1}} \end{pmatrix} \neq 0^\downarrow. \quad (52)$$

Рассмотрим отображение $\Xi: K \rightarrow K$, действие которого для произвольного элемента $\nu \in K, \nu_\mu^\downarrow = (\nu_0, \dots, \nu_{m-1})^T$ определяется равенством

$$\Xi(\nu) = \vec{\mu} \cdot \left(D_{n-1} \begin{pmatrix} \nu_0 \\ \nu_1 \\ \vdots \\ \nu_{m-1} \end{pmatrix} + D_{n-2} \begin{pmatrix} \nu_0^{\varkappa} \\ \nu_1^{\varkappa} \\ \vdots \\ \nu_{m-1}^{\varkappa} \end{pmatrix} + \dots + D_0 \begin{pmatrix} \nu_0^{\varkappa^{n-1}} \\ \nu_1^{\varkappa^{n-1}} \\ \vdots \\ \nu_{m-1}^{\varkappa^{n-1}} \end{pmatrix} \right).$$

Заметим, что Ξ есть эндоморфизм модуля ${}_R K$, и следовательно, в силу изоморфизма $\text{End}({}_R K) \cong K_{mn, mn}$ (см., например, [28]) условие (52) выполнено для всех ненулевых векторов $(c_0, \dots, c_{m-1})^T \in S^{(m)}$ тогда и только тогда, когда обратима матрица $\widehat{\Xi} = B$ линейного преобразования Ξ в базисе $\vec{\lambda} = (\lambda_0, \dots, \lambda_{mn-1})$ модуля ${}_R K$. Предложение 5 доказано.

2.4. Доказательство теоремы 8

Так как отображение $\text{Tr}_{\check{S}}^{\mathcal{K}}: \check{S}\mathcal{K} \rightarrow \check{S}\check{S}$ есть эпиморфизм модулей, то для любых элементов $\gamma \in RT_{\mathcal{K}}(\Psi), s \in S, \varepsilon \in \mathcal{K}$, где

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \psi_1x - \psi_0 \in \check{S}[x],$$

последовательность вида

$$u(i) = \text{Tr}_{\check{S}}^{\mathcal{K}}(\gamma^i \varepsilon) \circ s, \quad i \geq 0,$$

принадлежит семейству $L_S(\Psi)$. Действительно, для любого $i \in \mathbb{N}_0$ имеем:

$$\begin{aligned} (\Psi(x) \cdot u)(i) &= \text{Tr}_S^{\mathcal{K}}((\gamma^m - \sum_{j=0}^{m-1} \psi_j \gamma^j) \varepsilon) \circ s \\ &= \text{Tr}_S^{\mathcal{K}}(\Psi(\gamma) \varepsilon) \circ s = \text{Tr}_S^{\mathcal{K}}(0) \circ s = 0 \circ s = 0. \end{aligned}$$

Рассмотрим последовательность над $\check{S}$ вида $w(i) = \text{Tr}_S^{\mathcal{K}}(\gamma^i)$, $i \geq 0$. Покажем, что

$$w \neq 0. \quad (53)$$

Предположим противное. Тогда в силу линейности следа и условия $R \subset \check{S}$ след каждого элемента из $R[\gamma]$ равен нулю, т. е. выполняется условие

$$\forall \varepsilon \in R[\gamma]: \text{Tr}_S^{\mathcal{K}}(\varepsilon) = 0. \quad (54)$$

Далее нам понадобится следующее утверждение.

Теорема 15 ([26]). *Если $\Psi(x) \in \check{S}[x]$ — унитарный многочлен степени m , то следующие условия равносильны:*

- 1) $\Psi(x)$ — МП-многочлен,
- 2) существует единственный МП-многочлен $F(x) \in R[x]$ степени mn такой, что для некоторого многочлена $\Phi(x) \in \check{S}[x]$ выполняются равенства

$$F(x) = \Phi(x)\Psi(x) = \Psi(x)\Phi(x), \quad (55)$$

- 3) существует такой МП-многочлен $F(x) \in R[x]$ степени mn , что $\Psi(x)$ делит $F(x)$ справа,
- 4) существует такой МП-многочлен $F(x) \in R[x]$ степени mn , что $\Psi(x)$ делит $F(x)$ слева.

Заметим, что кольцо $R[\gamma]$ есть поле. Действительно, пусть $F(x) \in R[x]$ — МП-многочлен, удовлетворяющий (55). Тогда в силу условия $\gamma \in RT_{\mathcal{K}}(\Psi)$ для некоторых многочленов $\Phi(x), H(x) \in \mathcal{K}[x]$ имеют место равенства

$$F(x) = \Phi(x)\Psi(x) = \Phi(x)H(x)(x - \gamma)$$

в кольце $\mathcal{K}[x]$, т. е. γ — корень МП многочлена $F(x) \in R[x]$ в кольце $R[\gamma]$. Следовательно, $R[\gamma]$ — поле, так как $F(x)$ неприводим над R .

Напомним, что $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ — базис пространства ${}_R S$ и каждому элементу $\psi \in \check{S}$ однозначно соответствует матрица $A(\psi)$ преобразования ψ в данном базисе. Пусть $R_{mn, mn}$ — кольцо $mn \times mn$ матриц над R , а отображение $\Xi : \mathcal{K} \rightarrow R_{mn, mn}$ — изоморфизм колец, ставящий в соответствие элементу $(\phi_{ij})_{i,j=1}^m \in \mathcal{K}$ элемент $(A(\phi_{ij}))_{i,j=1}^m$.

Далее для натурального числа k через $\text{Tr}_R^{R_{k,k}}$ мы обозначаем функцию след из кольца матриц $R_{k,k}$ в кольцо R , результат действия которой на элементе $B \in R_{k,k}$ есть сумма диагональных элементов матрицы B . Тогда, используя стандартные рассуждения о подобии матриц над полем, можно показать, что для любого поля $P \subset R_{mn, mn}$, содержащего R и такого, что $|P| = q^{mn}$, при всех $B \in P$ справедливо равенство

$$E_{mn} \cdot \text{Tr}_R^{R_{mn, mn}}(B) = B + B^q + \dots + B^{q^{mn-1}}. \quad (56)$$

Ранее было показано, что $R[\gamma] \subset \mathcal{K}$ является полем. Тогда множество

$$P = \{\Xi(\varepsilon), \varepsilon \in R[\gamma]\} \subset R_{mn, mn},$$

также является полем, поскольку Ξ — изоморфизм.

Для произвольного $\varepsilon = (\phi_{ij})_{i,j=1}^m \in R[\gamma]$ имеют место равенства

$$\text{Tr}_R^{R_{mn, mn}}(\Xi(\varepsilon)) = \text{Tr}_R^{R_{n,n}}\left(\sum_{k=1}^m A(\phi_{kk})\right) = \text{Tr}_R^{R_{n,n}}\left(A\left(\sum_{k=1}^m \phi_{kk}\right)\right). \quad (57)$$

С учетом (23) и (54) находим

$$\text{Tr}_R^{R_{n,n}}\left(A\left(\sum_{k=1}^m \phi_{kk}\right)\right) = \text{Tr}_R^{R_{n,n}}(A(\text{Tr}_S^{\mathcal{K}}(\varepsilon))) = \text{Tr}_R^{R_{n,n}}(A(0)) = 0. \quad (58)$$

Таким образом, показано, что для любого элемента B поля $P \subset R_{mn, mn}$ из q^{mn} элементов выполняется равенство $\text{Tr}_R^{R_{mn, mn}}(B) = 0$. С учетом (56) последнее означает, что многочлен $E_{mn}x + E_{mn}x^q + \dots + E_{mn}x^{q^{mn-1}}$ степени q^{mn-1} имеет в поле P хотя бы q^{mn} различных корней. Получено противоречие. Следовательно, условие (53) выполнено.

Так как последовательность w над $\check{S}$ не является нулевой, то существует $i_0 \in \mathbb{N}_0$, удовлетворяющее условию

$$w(i_0) = \text{Tr}_S^{\mathcal{K}}(\gamma^{i_0}) \neq 0.$$

Положим $\eta = \gamma^{i_0}$. Существует такой элемент $s \in S$, что

$$\text{Tr}_S^{\mathcal{K}}(\eta) \circ s \neq 0.$$

Следовательно, последовательность $u(i) = \text{Tr}_S^{\mathcal{K}}(\gamma^i \eta) \circ s$ есть ненулевая ЛРП из семейства $L_S(\Psi)$. Заметим, что для скрученной МП ЛРП $v \in L_S(\Psi)$ существует такое $j \in \mathbb{N}_0$, что $v(i) = x^j u(i) = \text{Tr}_S^{\mathcal{K}}(\gamma^i(\gamma^j \eta))$, $i \in \mathbb{N}_0$. Для завершения доказательства теоремы осталось заметить, что $v(i) = \text{Tr}_S^{\mathcal{K}}(\gamma^i \varepsilon) \circ s$, где $\varepsilon = \gamma^j \eta$.

2.5. Доказательство следствия 9

Положим $\beta = \gamma^t$. Заметим, что для последовательности w выполняется условие

$$\forall i \in \mathbb{N}_0 : w(i) = \text{Tr}_S^{\mathcal{K}}(\beta^i \varepsilon) \circ s. \quad (59)$$

Так как $(t, \tau) = 1$, то период последовательности $w = v(ti)$ равен периоду последовательности v , т. е. равен τ . Далее, поскольку матрица β обладает свойством (**), то по теореме 7 для унитарного многочлена

$$\Phi(x) = \text{Det}(Ex - \beta) \in \check{S}[x]$$

степени m имеем $\Phi(\beta) = 0$. Отсюда с учетом (59) получаем $w \in L_S(\Phi)$. Следовательно, w — скрученная МП ЛРП порядка m с характеристическим многочленом $\Phi(x)$.

Рассмотрим случай, когда все коэффициенты многочлена $\Psi(x)$ попарно коммутируют. Согласно [25] для элемента γ вида

$$\gamma = \begin{pmatrix} 0 & e & 0 & \dots & 0 \\ 0 & 0 & e & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & e \\ \psi_0 & \psi_1 & \psi_2 & \dots & \psi_{m-1} \end{pmatrix} \quad (60)$$

имеет место включение $\gamma \in RT(\Psi)$. Так как все коэффициенты многочлена $\Psi(x)$ попарно коммутируют, коммутируют и все элементы матрицы (60), а следовательно, и все элементы матриц γ^t для всех $t \in \mathbb{N}_0$. Дальнейшее доказательство проводится с использованием рассуждений из первой части доказательства данного следствия.

2.6. Доказательство теоремы 11

Пусть $F(x) \in R[x]$ — такой МП-многочлен степени mn , что $\Psi(x) \in \text{MP}(F)$.

Для многочлена $H(x) = \sum_{j \geq 0} h_j x^j \in \mathcal{K}[x]$ и натурального числа $t \in \mathbb{N}$ положим

$$H^{(t)}(x) = \sum_{j \geq 0} h_j^k x^j,$$

т. е. многочлен $H^{(t)}(x)$ получается из многочлена $H(x)$ возведением каждого коэффициента в степень t .

Далее используем обозначение $\Psi_j(x) = \Psi^{(q^j)}(x)$, $j \in \overline{0, mn}$. Доказательство теоремы опирается на свойства многочленов $\Psi_j(x)$.

Лемма 16. *Имеет место равенство*

$$\Psi(x) = \Psi_{mn}(x). \quad (61)$$

Доказательство леммы 16. Пусть $\gamma \in RT_K(\Psi)$ — элемент вида (60). Так как многочлен $\Psi(x)$ обладает свойством (*) и свойством (**) одновременно, то согласно [25] существует такой многочлен $H(x) \in \mathcal{K}[x]$ вида

$$H(x) = \sum_{j=0}^{m-1} h_j x^j = x^{m-1} + \sum_{j=0}^{m-2} h_j x^j,$$

что

$$\Psi(x) = H(x)(x - \gamma) = (x - \gamma)H(x). \quad (62)$$

Лемма 17. *Пусть W — произвольное кольцо с единицей, $A(x)$ — унитарный многочлен степени m , все коэффициенты которого попарно коммутируют, и пусть для некоторого многочлена $B(x) \in W[x]$ и обратимого элемента δ кольца W выполнено равенство*

$$A(x) = B(x)(x - \delta) = (x - \delta)B(x). \quad (63)$$

Тогда все коэффициенты многочлена $B(x)$ попарно коммутируют. Кроме того, все коэффициенты многочлена $B(x)$ коммутируют с δ .

Доказательство леммы 17. Пусть $A(x) = \sum_{j=0}^m a_j x^j$. Заметим, что многочлен $B(x)$ унитарный. Пусть $B(x)$ имеет вид

$$B(x) = \sum_{j=0}^{m-1} b_j x^j = x^{m-1} + \sum_{j=0}^{m-2} b_j x^j.$$

Сначала покажем, что

$$b_0 b_j = b_j b_0, \quad j \in \overline{0, m-1}. \quad (64)$$

Считаем, что $m \geq 3$, так как в противном случае (64) выполнено в силу условия $b_{m-1} = e$. Из условия (63) находим

$$b_0\delta = \delta b_0, \quad b_{j-1} - b_j\delta = b_{j-1} - \delta b_j, \quad j \in \overline{1, m-1}.$$

Отсюда получаем

$$\delta b_j = b_j\delta, \quad j \in \overline{0, m-1}. \quad (65)$$

Используя равенство $a_0a_j = a_ja_0$ для $j \in \overline{1, m-1}$, находим

$$b_0\delta(b_{j-1} - b_j\delta) = (b_{j-1} - b_j\delta)b_0\delta, \quad j \in \overline{1, m-1}. \quad (66)$$

С учетом (65) перепишем (66) в виде

$$b_0b_{j-1}\delta - b_0b_j\delta^2 = b_{j-1}b_0\delta - b_jb_0\delta^2, \quad j \in \overline{1, m-1}. \quad (67)$$

При $j = m-1$ равенство (67) имеет вид

$$b_0b_{m-2}\delta - b_0\delta^2 = b_0b_{m-2}\delta - b_0\delta^2,$$

так как $b_{m-1} = e$. В силу обратимости элемента δ в кольце W находим

$$b_0b_{m-2} = b_{m-2}b_0. \quad (68)$$

Рассматривая равенство (67) для случая $j = m-3$, с учетом (68) приходим к условию $b_0b_{m-3} = b_{m-3}b_0$. Действуя аналогично для остальных j , приходим к (64).

Теперь покажем, что

$$b_jb_k = b_jb_k, \quad j, k \in \overline{0, m-1}. \quad (69)$$

Доказательство проведем индукцией по параметру $t = k + j$. База индукции для $t \leq 2$ следует из (64). Поэтому далее считаем, что $j > 0, k > 0$. Пусть утверждение верно для $t \leq l$. Докажем его для $t = l+1$. Если $k = 0$ или $j = 0$, то утверждение следует из (64). По условию $a_ja_k = a_ka_j$, т. е.

$$(b_{j-1} - b_j\delta)(b_{k-1} - b_k\delta) = (b_{k-1} - b_k\delta)(b_{j-1} - b_j\delta).$$

После преобразований получаем

$$\begin{aligned} & b_{j-1}b_{k-1} - b_{j-1}b_k\delta - b_j\delta b_{k-1} + b_j\delta b_k\delta \\ &= b_{k-1}b_{j-1} - b_k\delta b_{j-1} - b_{k-1}b_j\delta + b_k\delta b_j\delta. \end{aligned}$$

Пользуясь предположением индукции, свойством $\delta \in W^*$ и условием (65), находим $b_kb_j = b_jb_k$. Тем самым (69) доказано. Справедливость леммы 17 следует из (65) и (69). $\square$

Вернемся к доказательству леммы 16. Напомним, что имеет место (62). По п. 2 теоремы 6 элемент γ обратим в $\mathcal{K}$. Тогда по лемме 17 все коэффициенты многочлена $H(x)$ попарно коммутируют и коммутируют с γ . Следовательно,

$$\Psi_j(x) = H^{(q^j)}(x)(x - \gamma^{q^j}), \quad j \in \overline{0, mn}. \quad (70)$$

Пусть $v \in L_S(\Psi)$ — произвольная скрученная МП ЛРП. Тогда согласно теореме 8 существуют такие элементы $\epsilon \in \mathcal{K}, s \in S$, что $v(i) = \text{Tr}_S^{\mathcal{K}}(\gamma^i \epsilon) \circ s$ для всех $i \geq 0$. Так как для всех $j \in \overline{0, mn}$ числа q^j и $\tau = q^{mn} - 1$ взаимно просты и в силу (30) элемент γ обладает свойством (**), то по следствию 9 последовательности

$$v^{(j)}(i) = \text{Tr}_S^{\mathcal{K}}(\gamma^{q^j i} \epsilon) \circ s, \quad i \geq 0,$$

суть скрученные МП ЛРП порядка m . С учетом (70) находим

$$v^{(j)} \in L_S(\Psi_j), \quad j \in \overline{0, mn},$$

т. е. многочлены $\Psi_j(x)$ суть МП-многочлены.

По п. 2 теоремы 6 имеем $\gamma^{q^{mn}} = \gamma$. Тогда с учетом (70) находим, что

$$x - \gamma | \Psi(x), \quad x - \gamma | \Psi_{mn}(x), \quad (71)$$

т. е. многочлен $x - \gamma$ делит справа в кольце $\mathcal{K}[x]$ МП-многочлены $\Psi(x)$ и $\Psi_{mn}(x)$. Покажем, что последнее возможно тогда и только тогда, когда $\Psi(x) = \Psi_{mn}(x)$. Нам понадобится следующее утверждение.

Теорема 18 ([25]). Пусть $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$ — МП-многочлен. Тогда левый идеал

$$\check{S}[x]\Psi(x)$$

есть максимальный левый идеал кольца $\check{S}[x]$.

Напомним, что многочлены $A(x), B(x) \in \check{S}[x]$ называются взаимно простыми (слева), если существуют такие многочлены $U(x), V(x) \in \check{S}[x]$, что

$$U(x)A(x) + V(x)B(x) = e.$$

Из теоремы 18 следует, что для любого многочлена $A(x) \in \check{S}[x]$ либо $\Psi(x)$ делит $A(x)$ справа, либо $\Psi(x)$ взаимно прост с $A(x)$. В силу условия (71) МП-многочлены $\Psi(x)$ и Ψ_{mn} не взаимно просты. Следовательно, $\Psi(x)$ делит справа многочлен $\Psi_{mn}(x)$. Так как многочлены $\Psi(x)$

и $\Psi_{mn}(x)$ суть унитарные многочлены степени m , последнее возможно тогда и только тогда, когда $\Psi(x) = \Psi_{mn}(x)$. Лемма 16 доказана. $\square$

Для МП-многочлена $F(x) \in R[x]$ степени mn обозначим через $\text{MP}(F)$ множество МП-многочленов степени m над $\check{S}$, делящих $F(x)$ справа. Отметим, что в силу эквивалентности п. 1 и п. 2 теоремы 15 для двух различных МП-многочленов $F_1(x), F_2(x) \in R[x]$ степени mn справедливо равенство $\text{MP}(F_1) \cap \text{MP}(F_2) = \emptyset$.

Лемма 19. *Многочлены $\Psi_0(x), \Psi_1(x), \dots, \Psi_{mn-1}(x)$ суть попарно коммутирующие МП-многочлены из семейства $\text{MP}(F)$.*

Доказательство леммы 19. Ранее было показано, что $\Psi_j(x)$ есть МП-многочлен. Покажем, что $\Psi_j(x) | F(x)$. Из теоремы 15 и условия (62) следует, что существуют такие многочлены $\Phi(x), B(x) \in \mathcal{K}[x]$, что

$$F(x) = \Phi(x)\Psi(x) = B(x)(x - \gamma).$$

Так как $F(x)$ есть унитарный многочлен над полем R , то по лемме 17 все коэффициенты многочлена $B(x)$ попарно коммутируют и коммутируют с γ . Следовательно,

$$F(x) = F^{(q^j)}(x) = B^{(q^j)}(x)(x - \gamma^{q^j}), \quad j \in \overline{0, mn-1}.$$

С учетом условия (70) находим, что для каждого $j \in \overline{0, mn-1}$ многочлены $\Psi_j(x)$ не взаимно просты с многочленом $F(x)$. Следовательно, по теореме 18 выполняется условие $\Psi_j(x) | F(x)$, $j \in \overline{0, mn-1}$. Попарная коммутативность многочленов $\Psi_j, j \in \overline{0, mn-1}$, следует из условия (30). Лемма 19 доказана. $\square$

Лемма 20. *Многочлены $\Psi(x), \Psi_1(x), \dots, \Psi_{n-1}(x)$ попарно различны.*

Доказательство леммы 20. Предположим противное. Пусть

$$\Psi_i(x) = \Psi_k(x), \quad i, k \in \overline{0, n-1}, \quad i < k.$$

Без ограничения общности можно считать, что $i = 0$. Действительно, используя лемму 16, находим

$$\Psi(x) = \Psi_i^{(q^{mn-i})}(x) = \Psi_k^{(q^{mn-i})}(x) = \Psi_{k-i}(x).$$

Таким образом, $\Psi(x) = \Psi_0(x) = \Psi_k(x) = \Psi_{2k} = \dots = \Psi_{mk}$. Следовательно, в силу (70) многочлен $\Psi(x)$ имеет в $\mathcal{K}$ хотя бы $m+1$ различных корней $\gamma, \gamma^{q^k}, \dots, \gamma^{q^{km}}$, т. е. существуют многочлены $B_0(x), \dots,$

$B_m(x) \in \mathcal{K}[x]$, удовлетворяющие условиям

$$\Psi(x) = B_j(x)(x - \gamma^{q^{kj}}), \quad j \in \overline{0, m}. \quad (72)$$

Пусть $D(x) = \prod_{j \in \overline{0, m}} (x - \gamma^{q^{kj}})$. Наша цель — доказать, что

$$D(x) | \Psi(x). \quad (73)$$

Заметим, что если (73) будет доказано, то будет получено противоречие, так как $D(x)$ и $\Psi(x)$ суть унитарные многочлены и степень $D(x)$ больше степени $\Psi(x)$.

Докажем (73). При доказательстве будем использовать стандартные рассуждения, которые используются при обосновании свойств взаимно простых многочленов над коммутативными кольцами. В доказательстве теоремы 8 показано, что подкольцо $R[\gamma]$ кольца $\mathcal{K}$ есть поле. Тогда многочлены $x - \gamma, x - \gamma^{q^k}, \dots, x - \gamma^{q^{km}}$ суть взаимно простые многочлены над полем $R[\gamma]$. Следовательно, существуют такие многочлены $U_1(x), V_1(x) \in R[\gamma]$, что

$$U_1(x)(x - \gamma) + V_1(x)(x - \gamma^{q^k}) = e.$$

Умножив это равенство слева на $\Psi(x)$, получим

$$\Psi(x)U_1(x)(x - \gamma) + \Psi(x)V_1(x)(x - \gamma^{q^k}) = \Psi(x).$$

Напомним, что γ есть сопровождающая матрица многочлена $\Psi(x)$. Следовательно, с учетом (30), (72) и условия $U_1(x), V_1(x) \in R[\gamma]$ последнее равенство можно переписать в виде

$$\begin{aligned} & U_1(x)\Psi(x)(x - \gamma) + V_1(x)\Psi(x)(x - \gamma^{q^k}) \\ &= U_1(x)B_1(x)(x - \gamma^{q^k})(x - \gamma) + V_1(x)B_0(x)(x - \gamma)(x - \gamma^{q^k}) = \Psi(x). \end{aligned}$$

Поэтому существует многочлен $C_1(x) \in \mathcal{K}[x]$, для которого

$$\Psi(x) = C_1(x)(x - \gamma)(x - \gamma^{q^k}). \quad (74)$$

Если $m = 1$, то условие (73) доказано. Далее считаем, что $m \geq 2$. Многочлены $x - \gamma^{q^{2k}}$ и $(x - \gamma)(x - \gamma^{q^k})$ суть взаимно простые многочлены над полем $R[\gamma]$. Следовательно, существуют такие многочлены $U_2(x), V_2(x) \in R[\gamma]$, что

$$U_2(x)(x - \gamma^{q^{2k}}) + V_2(x)(x - \gamma)(x - \gamma^{q^k}) = e.$$

Умножив последнее равенство на $\Psi(x)$ слева, получим

$$\Psi(x)U_2(x)(x - \gamma^{q^{2k}}) + \Psi(x)V_2(x)(x - \gamma)(x - \gamma^{q^k}) = \Psi(x).$$

Так как многочлен $\Psi(x)$ коммутирует с $U_2(x)$ и с $V_2(x)$, то с учетом равенства (74) получим

$$\Psi(x) = C_2(x)(x - \gamma)(x - \gamma^{q^k})(x - \gamma^{q^{2k}}).$$

Продолжая действовать аналогично, придем к (73). Таким образом, получено противоречие. Лемма 20 доказана. $\square$

Лемма 21. *Имеет место разложение*

$$F(x) = \Psi_{n-1}(x)\Psi_{n-2}(x) \cdot \dots \cdot \Psi_0(x). \quad (75)$$

Доказательство леммы 21. Ранее было показано, что для МП-многочленов $\Psi_0(x), \Psi_1(x), \dots, \Psi_{n-1}(x)$ справедливы соотношения

$$\begin{aligned} \Psi_i(x)\Psi_j(x) &= \Psi_j(x)\Psi_i(x), \quad i, j \in \overline{0, n-1}, \\ \Psi_i(x) &\neq \Psi_j(x), \quad i, j \in \overline{0, n-1}, i \neq j, \\ \Psi_j &\in \text{MP}(F), \quad j \in \overline{0, n-1}. \end{aligned} \quad (76)$$

Напомним, что аннулятором в кольце $\check{S}[x]$ произвольной последовательности v над S называется множество многочленов над $\check{S}$, аннулирующих v :

$$\text{Ann}_{\check{S}[x]}(v) = \{A(x) \in \check{S}[x] : A(x)v = 0\}.$$

Далее нам понадобится следующее утверждение.

Теорема 22 ([8]). *Пусть v — скрученная МП ЛРП порядка m над S с характеристическим многочленом $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$. Тогда*

$$\text{Ann}_{\check{S}[x]}(v) = \check{S}[x]\Psi(x).$$

Пусть $F(x) = \Phi(x)\Psi(x)$, а v_1 — скрученная МП ЛРП из семейства $L_S(\Psi_1)$. Покажем, что $\Psi(x)v_1$ есть скрученная МП ЛРП из семейства $L_S(\Psi_1)$. По лемме 20 МП-многочлены $\Psi(x)$ и $\Psi_1(x)$ различны, следовательно, по теореме 22 имеет место неравенство $\Psi(x)v_1 \neq 0$. В дальнейшем для упрощения формул вместо $\Psi_j(x)$ будем писать Ψ_j для $j \in \overline{0, mn-1}$. С учетом условия (30) находим

$$\Psi_1 \cdot (\Psi \cdot v_1) = (\Psi_1 \cdot \Psi)v_1 = (\Psi \cdot \Psi_1)v_1 = \Psi \cdot (\Psi_1 \cdot v_1) = 0,$$

т. е. ненулевая последовательность $\Psi(x)v_1$ принадлежит семейству $L_S(\Psi_1)$. Таким образом, $\Psi(x)v_1$ — скрученная МП ЛРП.

По лемме 19 $\Psi_1(x) \in \text{MP}(F)$. Следовательно, $F(x)v_1 = 0$. Тогда

$$\Phi(x)(\Psi(x)v_1) = 0.$$

Так как $\Psi(x)v_1$ есть скрученная МП ЛРП из семейства $L_S(\Psi_1)$, то по теореме 22 существует такой многочлен $\Lambda_1(x) \in \check{S}[x]$ степени $m(n-2)$, что

$$\Phi(x) = \Lambda_1(x)\Psi_1(x).$$

Если $n = 2$, то $\Lambda_1 = e$, и лемма 21 доказана.

Далее считаем $n > 2$. Покажем, что многочлен $\Psi_2(x)$ делит $\Lambda_1(x)$ справа. Пусть v_2 — скрученная МП ЛРП из семейства $L_S(\Psi_2)$, тогда $\Psi_1\Psi v_2$ есть скрученная МП ЛРП из семейства $L_S(\Psi_2)$. Действительно, из равенства

$$\Psi_2 \cdot (\Psi \cdot v_2) = \Psi \cdot (\Psi \cdot v_2) = 0$$

следует, что $\Psi(x)v_2$ есть скрученная ЛРП из семейства $L_S(\Psi_2)$. Кроме того, $\Psi(x)v_2 \neq 0$ в силу леммы 20 и теоремы 22. Аналогично устанавливаем, что последовательность $\Psi_1(x)\Psi(x)v_2$ есть скрученная МП ЛРП из семейства $L_S(\Psi_2)$. Тогда

$$F(x)v_2 = \Lambda_1(x) \cdot (\Psi_1(x)\Psi(x)v_2) = 0.$$

Следовательно, по теореме 22 многочлен $\Psi_2(x)$ делит $\Lambda_1(x)$ справа, т. е. имеет место равенство

$$F(x) = \Lambda_2(x)\Psi_2(x)\Psi_1(x)\Psi(x)$$

для некоторого унитарного многочлена $\Lambda_2(x) \in \check{S}[x]$ степени $m(n-3)$.

Дальнейшее доказательство проводится аналогично. Лемма 21 доказана. $\square$

Перейдем к доказательству теоремы 11. Из равенства (75) с учетом условия (30) получаем

$$\Psi_{n-1}\Psi_{n-2}\dots\Psi_0 = F = F^{(q)} = \Psi_n\Psi_{n-1}\dots\Psi_1.$$

Тогда $\Psi_0(x) = \Psi_n(x)$, и

$$\Psi = \Psi_n = \Psi_{2n} = \dots = \Psi_{(m-1)n},$$

так как $\Psi_0(x) = \Psi(x)$. Следовательно, в силу (70) многочлен $\Psi(x)$ имеет корни $\gamma, \gamma^{q^n}, \dots, \gamma^{q^{n(m-1)}}$ в $\mathcal{K}$.

Проводя рассуждения, аналогичные тем, которые были использованы при обосновании условия (73), находим, что многочлен $\prod_{t=0}^{m-1} (x - \gamma^{q^{tn}})$ делит $\Psi(x)$ в кольце $\mathcal{K}[x]$. Следовательно,

$$\Psi(x) = \prod_{t \in \overline{0, m-1}} (x - \gamma^{q^{tn}}),$$

так как $\prod_{t=0}^{m-1} (x - \gamma^{q^{tn}})$ — унитарный многочлен и его степень равна m .

Напомним, что $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$. Тогда

$$\psi_0 = (-e)^{m-1} \gamma^{\frac{q^{mn}-1}{q^n-1}},$$

и $\gamma^{\frac{q^{mn}-1}{q^n-1}} \in \check{S}$. Положим

$$\xi = \gamma^{\frac{q^{mn}-1}{q^n-1}}. \quad (77)$$

Заметим, что для произвольного элемента $\mu \in \check{S}$ равенство $\mu\psi_0 = \psi_0\mu$ выполнено тогда и только тогда, когда $\mu\xi = \xi\mu$. Покажем, что с элементом ξ коммутируют только линейные комбинации над R степеней ξ , т. е. централизатор $C_{\check{S}}(\xi)$ элемента ξ в кольце $\check{S}$ равен $R[\xi]$.

Напомним, что $\vec{\alpha} = (\alpha_0, \dots, \alpha_{n-1})$ — базис векторного пространства ${}_R S$. Пусть $A(\xi)$ — матрица преобразования ξ в базисе $\vec{\alpha}$. В силу равенства $\text{ord } \xi = q^n - 1$ характеристический многочлен $\chi_{A(\xi)}(x) \in R[x]$ примитивен, а следовательно, неприводим над R и имеет степень n . Воспользуемся следующим (известным) утверждением.

Предложение 23 ([36]). Пусть $B \in R_{n,n}$ — матрица с минимальным многочленом $m_B(x)$. Тогда $C_{R_{n,n}}(B) = R[B]$ тогда и только тогда, когда

$$m_B(x) = \chi_B(x).$$

В силу неприводимости над R многочлена $\chi_{A(\xi)}(x) \in R[x]$ для матрицы $A(\xi)$ справедливо равенство $m_{A(\xi)}(x) = \chi_{A(\xi)}(x)$, и по предложению 23

$$C_{R_{n,n}}(A(\xi)) = R[A(\xi)].$$

Следовательно,

$$C_{\check{S}}(\psi_0) = C_{\check{S}}(\xi) = R[\xi] = R[\psi_0].$$

Тогда в силу (30) справедливо включение

$$\Psi(x) \in R[\psi_0]. \quad (78)$$

С учетом неприводимости характеристического многочлена $\chi_{A(\xi)}(x) \in R[x]$ над R находим, что множество $R[A(\xi)] = R[A(\psi_0)]$ есть поле. Следовательно, $R[\psi_0]$ является полем. Таким образом, S и $R[\psi_0]$ — два поля из q^n элементов в $\check{S}$. Тогда в силу изоморфизма (1) существует такой элемент $\phi \in \check{S}^*$, что

$$\phi R[\psi_0] \phi^{-1} = S.$$

С учетом (78) находим, что для некоторого многочлена $G(x) \in S[x]$ справедливо соотношение

$$\phi^{-1} \Psi(x) \phi = G(x) \in S[x],$$

т.е. многочлен $\Psi(x)$ является линеаризуемым МП-многочленом. Теорема 11 доказана.

Автор признателен В.В.Борисенко за ряд ценных замечаний, позволивших улучшить текст работы.

Список литературы

- [1] Куракин В.Л., Кузьмин А.С., Михалев А.В., Нечаев А.А., “Линейные рекуррентные последовательности над кольцами и модулями”, *Итоги науки и техники, Сер. Совр. матем. и ее прил., Алгебра-2*, **10** (1994), 1–130.
- [2] Нечаев А.А., “Код Кердока в циклической форме”, *Дискретная математика*, **1:4** (1989), 123–139.
- [3] Гольтованица М.А., Зайцев С.Н., Нечаев А.А., “Скрученные линейные рекуррентные последовательности максимального периода над кольцами Галуа”, *Фундам. и прикл. матем.*, **17:3** (2011), 5–23.
- [4] Куракин В.Л., Михалев А.В., Нечаев А.А., Цыпышев В.Н., “Линейные рекуррентные последовательности над абелевой группой и модулем”, *Итоги науки и техники, Сер. Совр. матем. и ее прил., Алгебра-15*, **74** (2000), 1–30.
- [5] Chen E., Tseng D., “The splitting subspace conjecture”, *Finite Fields Appl.*, **24** (2013), 15–28.
- [6] Zeng G., Yang Y., Han W., Fan S., “Word oriented cascade jump σ -LFSR”, *Lect. Notes Comput. Sci.*, **5527**, 2009, 127–136.
- [7] Goltvanitsa M.A., Nechaev A.A., Zaitsev S.N., “Skew LRS of maximal period over Galois rings”, *Математические вопросы криптографии*, **4:2** (2013), 59–72.
- [8] Goltvanitsa M.A., “Digit sequences of skew linear recurrences of maximal period over Galois rings”, *Математические вопросы криптографии*, **6:2** (2015), 19–27.
- [9] Goltvanitsa M.A., “The first digit sequence of skew linear recurrence of maximal period over Galois ring”, *Математические вопросы криптографии*, **7:3** (2016), 5–18.
- [10] Goltvanitsa M.A., “Equidistant filters based on skew ML-sequences over fields”, *Математические вопросы криптографии*, **9:2** (2018), 71–86.
- [11] Niederreiter H., “The multiple-recursive matrix method for pseudorandom number generation”, *Finite Fields Appl.*, **1** (1995), 3–30.

- [12] Tsaban B., Vishne U., “Efficient linear feedback shift registers with maximal period”, *Finite Fields Appl.*, **8**:2 (2002), 256–267.
- [13] 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>.
- [14] Zeng G., He K.C., Han W., “A trinomial type of σ -LFSR oriented toward software implementation”, *Science in China, Ser. F, Inf. Sci.*, **50**:3 (2007), 359–372.
- [15] Ghorpade S.R., Hasan S.U., Kumari M., “Primitive polynomials, Singer cycles, and word-oriented linear feedback shift registers”, *Des. Codes Cryptogr.*, **58**:2 (2011), 123–134.
- [16] Ghorpade S.R., Ram S., “Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields”, *Finite Fields Appl.*, **17**:5 (2011), 461–472.
- [17] Hasan S., Panario D., Wang Q., “Word-oriented transformation shift registers and their linear complexity”, *Lect. Notes Comput. Sci.*, **7280** (2012), 190–201.
- [18] Cohen S., Hasan S., Panario D., Wang Q., “An asymptotic formula for the number of irreducible transformation shift registers”, *Linear Algebra Appl.*, **484** (2015), 46–62.
- [19] Zaitcev S.N., “Description of maximal skew linear recurrences in terms of multipliers”, *Математические вопросы криптографии*, **5**:2 (2014), 57–70.
- [20] Зайцев С.Н., “Треугольный класс скрученных многочленов максимального периода”, *Проблемы передачи информации*, **52**:4 (2016), 84–93.
- [21] Bishoi S., Haran H., Hasan S., “A note on the multiple-recursive matrix method for generating pseudorandom vectors”, *Discr. Appl. Math.*, **222** (2017), 67–75.
- [22] Goltvanitsa M.A., “A construction of skew LRS of maximal period over finite fields based on the defining tuples of factors”, *Математические вопросы криптографии*, **5**:2 (2014), 37–46.
- [23] Гольтованица М.А., “Об одном классе скрученных линейных рекуррент максимального периода над кольцом Галуа”, *Системы высокой доступности*, **11**:3 (2015), 28–49.
- [24] Hassan S., Panario D., Wang Q., “Nonlinear vectorial primitive recursive sequences”, *Cryptogr. Commun.*, **10**:6 (2018), 1075–1090.
- [25] Goltvanitsa M.A., “Non-commutative Hamilton–Cayley theorem and roots of characteristic polynomials of skew maximal period linear recurrences over Galois rings”, *Математические вопросы криптографии*, **8**:2 (2017), 65–76.
- [26] Гольтованица М.А., “Методы построения скрученных линейных рекуррентных последовательностей максимального периода, базирующиеся на факторизации многочленов Галуа в кольце матричных многочленов”, *Математические вопросы криптографии*, **10**:4 (2019), 25–51.
- [27] McDonald B.R., *Finite Rings with Identity*, N. Y.: Markel Dekker, 1974, 429 pp.
- [28] Nechaev A.A., “Finite Rings with Applications”, *Handbook of Algebra*, **5**, Elsevier B.V., 2008, 213–320.
- [29] Sison V., “Bases of the Galois ring $\text{GR}(p^r, m)$ over the integer ring $\mathbb{Z}_{p^r}$ ”, <http://arxiv.org/pdf/1410.0289v1.pdf>.
- [30] Куракин В.Л., “Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа”, *Дискретная математика*, **6**:2 (1994), 88–100.
- [31] Lam T.Y., *A First Course in Noncommutative Rings*, N. Y.: Springer-Verlag, 1991, 398 pp.
- [32] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра*, **2**, М.: Гелиос АРВ, 2003, 414 с.
- [33] Ленг С., *Алгебра*, М.: Мир, 1968, 564 с.
- [34] Нечаев А. А., “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Мат. сб.*, **184**:3 (1993), 21–56.

- [35] Лидл Р., Нидеррайтер Г., *Конечные поля*, М.: Мир, 1988, 830 с.
- [36] Супруненко Д.А., Тышкевич Р.И., *Перестановочные матрицы*, Минск: Наука и техника, 1966, 104 с.