Math-Net.Ru

Общероссийский математический портал

М. А. Гольत्वаница, Методы построения скрученных линейных рекуррентных последовательностей максимального периода, базирующиеся на факторизации многочленов Галуа в кольце матричных многочленов, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 4, 25–51

DOI: <https://doi.org/10.4213/mvk306>

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: 44.207.124.84

26 апреля 2023 г., 16:49:48

**Методы построения скрученных линейных
рекуррентных последовательностей максимального
периода, базирующиеся на факторизации
многочленов Галуа в кольце матричных
многочленов**

М. А. Гольтваница

ООО «Центр сертификационных исследований», г. Москва

Получено 29.IV.2019

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 и $\check{S}$ — кольцо эндоморфизмов модуля ${}_R S$. Последовательность v над S , удовлетворяющую закону рекурсии

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

будем называть *скрученной линейной рекуррентной последовательностью над S с характеристическим многочленом $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$* . Максимально возможный период последовательности такого вида равен $\tau = (q^{mn} - 1)p^{d-1}$. В работе предлагаются новые методы построения многочленов $\Psi(x)$, задающих законы рекурсии для скрученных линейных рекуррентных последовательностей максимального периода. Данные методы основаны на поиске в кольце $\check{S}[x]$ делителей классических многочленов Галуа над R периода τ .

Ключевые слова: кольцо Галуа, автоморфизм Фробениуса, последовательность максимального периода, скрученная ЛРП, матричный многочлен, факторизация

Methods of construction of skew linear recurrent sequences with maximal period based on the Galois polynomials factorization in the ring of matrix polynomials

M. A. Goltvanitsa

LLC «Certification Research Center», Moscow

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

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

is called a *skew LRS over S with a characteristic polynomial $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$* . The maximal period $T(v)$ of such sequence equals $\tau = (q^{mn} - 1)p^{d-1}$. In this article we propose some new methods for construction the polynomials $\Psi(x)$, which define the recursion laws of skew linear recurrent sequences of maximal period. These methods are based on the search in $\check{S}[x]$ the divisors for classic Galois polynomials of period τ over R .

Keywords: Galois ring, Frobenius automorphism, ML-sequence, skew LRS, matrix polynomial, factorization

1. Введение. Основные результаты

Всюду 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 [2], что группа $\text{Aut}(S/R)$ автоморфизмов кольца S над R есть циклическая группа порядка n . Пусть σ — образующий элемент данной 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 по дистрибутивности из тождества

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

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

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

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

$$\check{S} \cong \text{End}({}_R S) \cong R_{n,n}, \quad (1.1)$$

где $R_{n,n}$ — кольцо $n \times n$ матриц над R .

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

$$\psi \cdot s = \psi(s).$$

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

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

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 справедливо равенство $\Psi(x)v = 0$ для некоторого унитарного многочлена

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \dots - \psi_0 \in \check{S}[x] \quad (1.2)$$

степени m , называемого *характеристическим многочленом ЛРП v* , так что последовательность v удовлетворяет закону рекурсии

$$\forall i \in \mathbb{N}_0 : \quad v(i+m) = \psi_{m-1}(v(i+m-1)) + \dots + \psi_0(v(i)). \quad (1.3)$$

Обозначим через $L_S(\Psi)$ множество всех ЛРП v над S с характеристическим многочленом $\Psi(x)$. В случае когда $\Psi(x) \in S[x]$, многочлен $\Psi(x)$ и последовательности из семейства $L_S(\Psi)$ будем называть *классическими*.

Предложение 1 ([3]). Пусть v — скрученная ЛРП порядка m над S . Тогда для периода $T(v)$ последовательности v имеет место оценка

$$T(v) \leq \tau = (q^{nm} - 1)p^{d-1}.$$

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 $L_S(\Psi)$ найдется скрученная МП ЛРП порядка m над S .

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

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

называемая *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 (1.3), тогда и только тогда, когда столбцы координат $v^\downarrow(i)$ членов этой последовательности в базисе $\vec{\alpha}$ удовлетворяют соотношению

$$\forall i \in \mathbb{N}_0 : v^\downarrow(i+m) = A(\psi_{m-1})v^\downarrow(i+m-1) + \dots + A(\psi_0)v^\downarrow(i). \quad (1.4)$$

Всюду далее для неотрицательных целых чисел a, b , $a \leq b$, через $\overline{a, b}$ мы обозначаем множество $\{a, a+1, \dots, b\}$. Согласно (1.1) матрицы $A_s = A(\psi_s) \in R_{n \times n}$, $s \in \overline{0, m-1}$, в (1.4) могут быть произвольными, и закон рекурсии (1.4) можно записать компактнее:

$$v^\downarrow(i+m) = A_{m-1}v^\downarrow(i+m-1) + \dots + A_0v^\downarrow(i), \quad A_0, \dots, A_{m-1} \in R_{n,n}, \quad i \geq 0. \quad (1.5)$$

Соотношение (1.5) будем называть *законом рекурсии скрученной ЛРП v в матричном виде*, а многочлен

$$Ex^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0 \in R_{n,n}[x] \quad (1.6)$$

— *характеристическим многочленом ЛРП v в матричном виде*. В (1.6) и всюду далее E — единичная $n \times n$ матрица над кольцом R .

В настоящей работе предлагаются новые методы построения МП-многочленов над $\check{S}$, позволяющие вырабатывать скрученные МП ЛРП. Интерес к классу скрученных ЛРП с точки зрения криптографии обусловлен прежде всего тем, что он включает в себя классические ЛРП и значительно превосходит множество классических ЛРП по мощности [5]. Данное обстоятельство приводит к тому, что порой удается построить скрученные МП ЛРП, подходящие для программной реализации и обладающие конструктивными преимуществами по сравнению с классическими ЛРП [6, 7]. В то же время, как показывают результаты работ [3, 8–10], к скрученным МП ЛРП применимы стандартные методы усложнения, которые позволяют получать псевдослучайные последовательности, имеющие лучшие криптографические характеристики по сравнению с псевдослучайными последовательностями, полученными из классических МП ЛРП того же порядка.

Отметим, что, хотя задача конструктивного описания всех МП-многочленов над $\check{S}$ не решена, в настоящий момент предложено несколько подходов к построению скрученных МП ЛРП и МП-многочленов над $\check{S}$, представляющих интерес для криптографических приложений. Для удобства ссылок и сравнения наших результатов с полученными ранее далее приводим краткий обзор исследований по данному направлению.

В случае когда S — поле, скрученные МП ЛРП изучались в [6, 11–16]. В отечественной литературе скрученные МП ЛРП исследовались в фундаментальной статье [4]. Отметим, что в указанных работах законы рекурсии скрученных МП ЛРП были найдены лишь в матричном виде над полями, преимущественно с использованием методов перебора. Первый результат в этом направлении — скрученная МП ЛРП периода $2^{256} - 1$ порядка 16 с трехчленным законом рекурсии над модулем $\check{S}$, где $S = \text{GF}(2^{16})$, построенная в [4]. При этом стоит заметить, что не существует классических трехчленных МП ЛРП порядка 16 над полем $\text{GF}(2^{16})$. Данный результат свидетельствует о том, что переход от классических ЛРП к скрученным позволяет получить конструктивные преимущества, например существование трехчленных ЛРП максимального периода. Скрученные МП ЛРП с трехчленными законами рекурсии, ориентированными на быструю выработку знаков, изучались также в [6]. В [12] предлагается алгоритм построения скрученных МП

ЛРП над полем $\text{GF}(2^n)$ с характеристическим многочленом вида

$$\Psi(x) = x^m - \xi(r_{m-1}x^{m-1} - \dots - r_1x - r_0), \quad (1.7)$$

где $\xi \in \check{S}$, $r_0, \dots, r_{m-1} \in \text{GF}(2)$. Скрученные МП ЛРП с характеристическими многочленами вида (1.7) изучались также в [17, 18]. Стоит отметить, что все перечисленные выше работы в значительной мере способствовали изучению классов скрученных МП ЛРП, ориентированных на быструю выработку знаков и подходящих для удобной программной реализации на современных ЭВМ. Однако методы построения классов скрученных МП ЛРП и МП-многочленов над $\check{S}$, упомянутые в этих статьях, относились к случаю, когда S — поле, и не позволяли строить последовательности гарантированного ранга. Далее под рангом последовательности над S мы всегда понимаем ее ранг как ЛРП над модулем ${}_S S$ (см., например, [1]).

Систематическое изучение свойств скрученных МП ЛРП над кольцами Галуа было начато в [3], где в частности исследовались ранги скрученных МП ЛРП. Следующее утверждение дает первый конструктивный способ построения из одной скрученной МП ЛРП над кольцом Галуа целого класса скрученных МП ЛРП.

Теорема 2 ([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 — 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 — скрученная МП ЛРП порядка t над S , то $\psi \in \check{S}^*$.

Если выполнены условия п. 1 теоремы 2, а v — классическая МП ЛРП порядка t над кольцом S , т. е. $\Psi(x) \in S[x]$, то назовем 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 [3]. Множество линеаризуемых МП-многочленов полностью описано в [3], там же доказана формула для его мощности и вычислены ранги скрученных МП ЛРП с характеристическими многочленами из данного множества.

Результаты, позволяющие строить классы нелинеаризуемых МП-многочленов в матричной форме, получены в [7, 19, 20]. Позднее один из результатов [7] в частном случае был повторен в [21].

Альтернативный подход к синтезу скрученных МП ЛРП предложен в [22]. Суть его заключается в том, что сначала строится не многочлен над $\check{S}$, который задает закон рекурсии скрученной МП ЛРП, а, наоборот, строится некоторая последовательность, аннулятор которой гарантированно содержит МП-многочлены над $\check{S}$.

Отдельно выделим работу [23], где впервые получены условия на вид МП-многочлена $\Psi(x) \in \check{S}[x]$, при которых достигается максимальный ранг произвольной скрученной МП ЛРП из семейства $L_S(\Psi)$. Из [3] известно, что для ранга $\text{rank}_S v$ скрученной МП ЛРП v порядка m над S справедливы неравенства

$$m \leq \text{rank}_S v \leq nm. \quad (1.8)$$

Отметим, что для скрученных МП ЛРП левое неравенство в (1.8) является строгим всегда (за исключением «тривиального» случая, когда v — классическая МП ЛРП над модулем ${}_S S$), а правое неравенство иногда достижимо [3]. В [23] изучен класс многочленов над $\check{S}$ вида

$$\Psi(x) = x^m - \sum_{j \in W_1} h_j x^j - \sum_{j \in W_2} h_j \sigma^l x^j \in \check{S}[x], \quad (1.9)$$

где

$$l \in \overline{1, n-1}, \quad h_j \in S, \quad W_1, W_2 \subset \overline{0, m-1}, \quad W_1 \cap W_2 = \emptyset, \quad W_2 \neq \emptyset.$$

Там же показано, что если v — скрученная МП ЛРП с характеристическим многочленом (1.9), то v является нелинеаризуемой, обладает единственным минимальным многочленом над S и справедливо равенство $\text{rank}_S v = \frac{mn}{(n,l)}$, где l — параметр из (1.9) и через (n, l) обозначен наибольший общий делитель чисел n и l . Таким образом, чтобы гарантировать максимально возможный ранг скрученных МП ЛРП с характеристическим многочленом (1.9), достаточно выбирать параметр l взаимно простым с n . Отметим, что согласно [8–10, 24] использование стандартных методов усложнения ЛРП позволяет получать последовательности с максимальными рангом и периодом при применении к скрученным МП ЛРП максимального ранга.

Перейдем к основным результатам данной работы. Приведем определения, которые будут использоваться далее. Для периода многочлена $G(x)$ над S используется стандартное обозначение $T(G)$, [2]. Напомним, что для периода $T(F)$ унитарного многочлена

$$F(x) = x^{mn} - f_{mn-1}x^{mn-1} - \dots - f_1x - f_0 \in R[x] \quad (1.10)$$

степени mn справедливо неравенство

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

В случае когда в последнем неравенстве достигается равенство, многочлен $F(x)$ будем называть *многочленом максимального периода* (МП-многочленом) над R . Отметим, что всякий МП-многочлен над R является *многочленом Галуа*, т.е. его образ при эпиморфизме $R \rightarrow R/pR$ является неприводимым многочленом над полем [2]. В настоящей работе исследуются методы построения и размножения МП-многочленов вида (1.2) над $\check{S}$, базирующиеся на идее нахождения в кольце $\check{S}[x]$ делителей МП-многочленов вида (1.10).

Будем говорить, что многочлен $A(x) \in \check{S}[x]$ *делит справа* многочлен $B(x) \in \check{S}[x]$ (в кольце $\check{S}[x]$), если существует такой многочлен $C(x) \in \check{S}[x]$, что $B(x) = C(x)A(x)$. Аналогично определяется делимость слева. Отметим, что в силу некоммутативности кольца $\check{S}[x]$ из равенства $B(x) = C(x)A(x)$, вообще говоря, не следует равенство $B(x) = A(x)D(x)$ для некоторого многочлена $D(x) \in \check{S}[x]$.

Основой для получения всех дальнейших результатов является следующее утверждение.

Теорема 3. *Если $\Psi(x) \in \check{S}[x]$ — унитарный многочлен степени t , то следующие условия равносильны:*

- 1) $\Psi(x)$ — МП-многочлен.
- 2) *Существует единственный МП-многочлен $F(x) \in R[x]$ степени mn , удовлетворяющий для некоторого многочлена $\Phi(x) \in \check{S}[x]$ равенствам*

$$F(x) = \Phi(x)\Psi(x) = \Psi(x)\Phi(x). \quad (1.11)$$

- 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.*

Для МП-многочлена $F(x) \in R[x]$ степени mn обозначим через $\text{MP}(F)$ множество МП-многочленов степени t над $\check{S}$, делящих $F(x)$ справа. Отметим, что в силу эквивалентности п. 1 и п. 2 теоремы 3 для двух различных МП-многочленов $F_1(x), F_2(x) \in R[x]$ степени mn справедливо равенство

$$\text{MP}(F_1) \cap \text{MP}(F_2) = \emptyset.$$

Напомним, что n есть степень расширения кольца S над R . В случае, когда $n = 2$, теорема 3 указывает следующий способ построения МП-многочленов над $\check{S}$.

Следствие 4. Если $n = 2$, $F(x) \in R[x]$ — МП-многочлен степени mn и для некоторых унитарных многочленов $\Psi(x), \Phi(x) \in \check{S}[x]$ степени m выполнено равенство

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

то $\Phi(x), \Psi(x)$ есть МП-многочлены над $\check{S}$.

Таким образом, в случае когда $n = 2$ и МП-многочлены $F(x) \in R[x]$ и $\Psi(x) \in \check{S}[x]$ таковы, что $\Psi(x)$ делит $F(x)$ справа, можно построить новый МП-многочлен $\Phi(x) \in \check{S}[x]$, вычислив его как частное от деления $F(x)$ на $\Psi(x)$ в кольце $\check{S}[x]$. Отметим, что в ряде случаев (см., например, [7], [23]) по МП-многочлену $F(x) \in R[x]$ степени mn удается построить такой МП-многочлен $\Psi(x)$, что $\Psi(x)$ делит $F(x)$ справа в кольце $\check{S}[x]$.

Приведем пример использования следствия 4 для построения МП-многочленов в матричном виде. Пусть $R = \text{GF}(2)$ — поле мощности 2. Рассмотрим многочлен $F(x) = x^6 + x^5 + 1 \in R[x]$. Несложно убедиться в том, что $F(x)$ есть МП-многочлен над R . Далее отождествим многочлен $F(x)$ с многочленом $E \cdot F(x)$ над $R_{2,2}(x)$, имеющим вид

$$E \cdot F(x) = \begin{pmatrix} 10 \\ 01 \end{pmatrix} x^6 + \begin{pmatrix} 10 \\ 01 \end{pmatrix} x^5 + \begin{pmatrix} 10 \\ 01 \end{pmatrix} \in R_{2,2}[x]. \quad (1.12)$$

Рассмотрим многочлен $\Psi(x) \in R_{2,2}[x]$ вида

$$\Psi(x) = \begin{pmatrix} 10 \\ 01 \end{pmatrix} x^3 + \begin{pmatrix} 00 \\ 11 \end{pmatrix} x^2 + \begin{pmatrix} 01 \\ 10 \end{pmatrix} x + \begin{pmatrix} 01 \\ 11 \end{pmatrix}. \quad (1.13)$$

Несложно проверить, что $\Psi(x)$ является МП-многочленом из семейства $\text{MP}(F)$. Вычислим частное $\Phi(x)$ от деления многочлена (1.12) на многочлен (1.13) справа в кольце $R_{2,2}[x]$

$$\Phi(x) = \begin{pmatrix} 10 \\ 01 \end{pmatrix} x^3 + \begin{pmatrix} 10 \\ 10 \end{pmatrix} x^2 + \begin{pmatrix} 01 \\ 10 \end{pmatrix} x + \begin{pmatrix} 11 \\ 10 \end{pmatrix}. \quad (1.14)$$

По следствию 4 многочлен (1.14) есть МП-многочлен в матричной форме, кроме того, несложно проверить, что выполнено равенство

$$E \cdot F(x) = \Phi(x)\Psi(x) = \Psi(x)\Phi(x).$$

Отметим также, что многочлены $\Psi(x)$ и $\Phi(x)$ являются нелинеаризуемыми, так как не все их ненулевые коэффициенты обратимы в $R_{2,2}$ [7].

Приведем еще один наглядный пример факторизации МП-многочленов над R в кольце $\check{S}[x]$. Нам понадобится следующий результат.

Теорема 5 ([7]). Пусть e — нейтральный элемент кольца R . Тогда если (1.10) есть МП-многочлен над R , то многочлен

$$A(x) = Ex^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0 \in R_{n,n}[x], \quad (1.15)$$

где

$$A_0 = \begin{pmatrix} 0 & e & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e \\ f_0 & f_m & \dots & f_{(n-1)m} \end{pmatrix}, A_t = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \\ f_t & \dots & f_{(n-1)m+t} \end{pmatrix}, 1 \leq t < m, \quad (1.16)$$

есть нелинеаризуемый МП-многочлен в матричной форме.

Пусть, как и в предыдущем примере, $R = \text{GF}(2)$ — поле мощности 2 и $F(x) = x^6 + x + 1 \in R[x]$ — МП-многочлен над R . Рассмотрим многочлен $E \cdot F(x)$ над $R_{2,2}(x)$:

$$E \cdot F(x) = \begin{pmatrix} 10 \\ 01 \end{pmatrix} x^6 + \begin{pmatrix} 10 \\ 01 \end{pmatrix} x + \begin{pmatrix} 10 \\ 01 \end{pmatrix} \in R_{2,2}[x]. \quad (1.17)$$

Построим многочлен $\Psi(x)$ в матричном виде способом, указанным в теореме 5, по многочлену $F(x)$:

$$\Psi(x) = \begin{pmatrix} 10 \\ 01 \end{pmatrix} x^3 + \begin{pmatrix} 00 \\ 10 \end{pmatrix} x + \begin{pmatrix} 01 \\ 10 \end{pmatrix}. \quad (1.18)$$

В данном случае, как несложно убедиться, частное от деления многочлена (1.17) на многочлен (1.18) совпадает с многочленом (1.18), т. е. имеет место равенство

$$E \cdot F(x) = \Psi(x) \cdot \Psi(x).$$

Данный пример демонстрирует проявление эффекта, который возможен только в некоммутативном кольце, а именно: МП-многочлен $F(x)$ над R имеет в кольце $\check{S}[x]$ кратные множители, но не имеет кратных корней в $\check{S}$ (отсутствие кратных корней у многочлена $F(x)$ в кольце $\check{S}$ может быть показано напрямую и следует из п. 5 теоремы 2 [25]).

Обозначим через $\check{S}[x]^*$ мультипликативную группу кольца $\check{S}[x]$. Следующая теорема указывает возможность использования внутренних автоморфизмов кольца $\check{S}[x]$ при построении МП-многочленов над $\check{S}$.

Теорема 6. Пусть $\Psi(x) \in \text{MP}(F)$. Если $U(x) \in \check{S}^*[x]$, то многочлен

$$\Psi^{(U)}(x) = U^{-1}(x)\Psi(x)U(x) \quad (1.19)$$

есть МП-многочлен тогда и только тогда, когда $\Psi^{(U)}(x)$ — унитарный многочлен степени m . При этом

$$\Psi^{(U)}(x) \in \text{MP}(F).$$

Теорема 6 дает удобный способ размножения МП-многочленов, позволяющий по одному МП-многочлену строить целую серию МП-многочленов. Достаточные условия, при которых применение теоремы 6 становится возможным, указаны в следующем предложении.

Предложение 7. Пусть $\Psi(x) \in \check{S}[x]$ — МП-многочлен вида (1.2), $U(x)$ — обратимый многочлен над $\check{S}$. Положим

$$k = \max\{t \in \overline{0, m-1} : \psi_t \notin R\}.$$

Тогда при выполнении любого из условий

- 1) $k + \deg U(x) + \deg U^{-1}(x) < m$,
- 2) R — поле, $n = 2$ и $k + 2\deg U(x) < m$,

многочлен $\Psi^{(U)}(x)$ есть МП-многочлен степени m над $\check{S}$.

Заметим, что предложение 7 является обобщением теоремы 2: способ построения МП-многочленов, указанный в теореме 2, совпадает со способом, описанным в п. 1 предложения 7, если $\deg U(x) = 0$.

Напомним, что $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ — фиксированный базис свободного модуля ${}_R S$, и для элемента $\psi \in \check{S}$ через $A(\psi) \in R_{n,n}$ обозначена матрица эндоморфизма ψ в базисе $\vec{\alpha}$.

Далее для произвольной матрицы A через A^T обозначается транспонированная матрица.

Каждому многочлену $\Psi(x) = \sum_{j \geq 0} \psi_j x^j \in \check{S}[x]$ однозначно соответствует многочлен $A_\Psi(x) = \sum_{j \geq 0} A(\psi_j) x^j$. Положим

$$\Psi^T(x) = \sum_{j \geq 0} \phi_j x^j \in \check{S}[x], \quad A(\phi_j) = A(\psi_j)^T, \quad j \geq 0.$$

Предложение 8. Если $F(x)$ — МП-многочлен степени m над R , то

$$\Psi(x) \in \text{MP}(F) \Leftrightarrow \Psi^T(x) \in \text{MP}(F).$$

Для элемента $\phi = \sum_{j=0}^{n-1} s_j \sigma^j \in \check{S}$ и многочлена $\Phi(x) = \sum_{j \geq 0} \phi_j x^j$ положим

$$\phi^{[*]} = \sum_{j=0}^{n-1} \sigma^{n-j}(s_j) \sigma^{n-j}, \quad \Phi^{[*]}(x) = \sum_{j \geq 0} \phi_j^* x^j.$$

Напомним (см., например, [26]), что биективное отображение $\nu: P \rightarrow P$ произвольного кольца P называется *инволюцией*, если для всех $t_1, t_2 \in P$ выполнены условия

$$\nu(\nu(t_1)) = t_1, \quad \nu(t_1 + t_2) = \nu(t_1) + \nu(t_2), \quad \nu(t_1 \cdot t_2) = \nu(t_2) \cdot \nu(t_1).$$

Отметим, что операция транспонирования является инволюцией кольца матриц. Как будет показано далее (см. лемму 14), соответствие $\phi \rightarrow \phi^{[*]}$ есть инволюция скрученного группового кольца $\check{S}$. Следующее предложение указывает возможность использования этой инволюции при построении новых МП-многочленов из заданных.

Предложение 9. Если выполнены условия предложения 8, то

$$\Psi(x) \in \text{MP}(F) \Leftrightarrow \Psi^{[*]} \in \text{MP}(F).$$

Унитарный многочлен над $\check{S}$ назовем *реверсивным*, если его свободный член обратим. Для реверсивного многочлена $\Psi(x) = \sum_{j \geq 0} \psi_j x^j \in \check{S}[x]$ положим

$$\Psi^*(x) = \psi_0^{-1} \sum_{j \geq 0} \psi_{m-j} x^j, \quad \Psi^{(*)}(x) = \sum_{j \geq 0} \psi_{m-j} \psi_0^{-1} x^j.$$

Предложение 10. Если выполнены условия предложения 8, то

- 1) $\Psi(x) \in \text{MP}_S(F) \Leftrightarrow \Psi^* \in \text{MP}(F^*),$
- 2) $\Psi(x) \in \text{MP}_S(F) \Leftrightarrow \Psi^{(*)} \in \text{MP}(F^*).$

Следуя [30], многочлены $\Psi^*(x)$ и $\Psi^{(*)}(x)$ назовем соответственно *левым двойственным* и *правым двойственным* к $\Psi(x)$.

Отметим, что для многочленов $\Psi^*(x)$ и $\Psi^{(*)}(x)$ справедливы формальные равенства

$$\Psi^*(x) = \psi_0^{-1} x^m \Psi\left(\frac{1}{x}\right), \quad \Psi^{(*)}(x) = x^m \Psi\left(\frac{1}{x}\right) \psi_0^{-1}, \quad (1.20)$$

т. е. эти многочлены могут быть получены путем формального вычисления значения определенных многочленов в точке $\frac{1}{x}$. Следующая теорема развивает эту идею и позволяет по МП-многочленам над $\check{S}$ строить МП-многочлены большей степени.

Теорема 11. Пусть R — поле, $F(x) \in R[x]$ — МП-многочлен степени mn с корнем ϑ в расширении $K = \text{GF}(q^{mn})$ поля R , $\Psi(x)$ — МП-многочлен из семейства $\text{MP}(F)$, имеющий вид

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \dots - \psi_1x - \psi_0,$$

и $h(x), g(x) \in R[x]$ — взаимно простые многочлены степеней k_1 и k_2 соответственно. Пусть $k = \max\{k_1, k_2\}$ и $\Lambda(x) = \sum_{j=0}^{mk} \lambda_j x^j \in \check{S}[x]$ — многочлен, определенный следующим образом:

$$\Lambda(x) = h(x)^m - \sum_{j=0}^{m-1} \psi_j h(x)^j g(x)^{m-1-j}. \quad (1.21)$$

Тогда

$$(\lambda_{mk})^{-1} \Lambda(x) \quad (1.22)$$

есть МП-многочлен над $\check{S}$, если и только если

$$h(x) - \vartheta \cdot g(x) \in K[x] \quad (1.23)$$

есть МП-многочлен над K .

Отметим, что по аналогии с формальными равенствами (1.20) для многочлена $\Lambda(x)$ вида (1.21) справедливо формальное равенство

$$\Lambda(x) = \Psi\left(\frac{h(x)}{g(x)}\right) g(x)^m.$$

Заметим также, что теорема 11 в общем виде может быть доказана для случая, когда R — произвольное кольцо Галуа, а $F(x)$ — многочлен Галуа. Более жесткие условия в теореме 11 наложены для упрощения формулировки и сокращения объема доказательства.

Следует подчеркнуть, что теорема 11 сводит задачу проверки того, что многочлен (1.22) является МП-многочленом над некоммутативным кольцом $\check{S}[x]$, к задаче проверки того, что многочлен (1.23) является МП-многочленом над полем.

2. Доказательства

Далее нам понадобятся конструкции доказательства предложения 1 из [3]. Поэтому для удобства приводим это доказательство полностью.

2.1. Доказательство предложения 1

Несложно видеть, что последовательность $v \in S^{(1)}$ есть скрученная МП ЛРП порядка m с характеристическим многочленом $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$ тогда и только тогда, когда столбцы координат $v^\downarrow(i)$ элементов $v(i)$ последовательности v в базисе $\vec{\alpha}$ удовлетворяют соотношению

$$v^\downarrow(i+m) = A(\psi_{m-1})v^\downarrow(i+m-1) + \dots + A(\psi_0)v^\downarrow(i), \quad i \in \mathbb{N}_0. \quad (2.1)$$

Пусть $v^\downarrow$ — последовательность векторов из $R^{(n)}$, удовлетворяющая закону рекурсии (2.1). Введем обозначения

$$\begin{aligned} \vec{v}(i) &= (v_0(i), v_1(i), \dots, v_{n-1}(i)) = (v^\downarrow(i))^T, \\ v^\downarrow(i) &= (\vec{v}(i), \vec{v}(i+1), \dots, \vec{v}(i+(m-1)))^T. \end{aligned} \quad (2.2)$$

Напомним, что E есть единичная $n \times n$ матрица над R и $A_j = A(\psi_j)$ для всех $j \in \overline{0, m-1}$. Тогда для матрицы

$$A_\Psi = \begin{pmatrix} 0 & E & 0 & \dots & 0 \\ 0 & 0 & E & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & E \\ A_0 & A_1 & A_2 & \dots & A_{m-1} \end{pmatrix}_{mn \times mn} \quad (2.3)$$

над кольцом R справедливы равенства

$$A_\Psi v^\downarrow(i) = v^\downarrow(i+1), \quad A_\Psi^k v^\downarrow(i) = v^\downarrow(i+k), \quad k \in \mathbb{N}. \quad (2.4)$$

Пусть $F(x) = x^{mn} - f_{mn-1}x^{mn-1} - \dots - f_1x - f_0 = \chi_A(x) \in R[x]$ — характеристический многочлен матрицы A . Тогда по теореме Гамильтона–Кэли (см., например, [28]) имеет место соотношение

$$A_\Psi^{mn} = f_{mn-1}A_\Psi^{mn-1} + \dots + f_1A_\Psi + f_0E.$$

Умножая обе части последнего равенства на $v^\downarrow(i)$ и применяя (2.4), получаем

$$v^\downarrow(i+mn) = f_{mn-1}v^\downarrow(i+mn-1) + \dots + f_0v^\downarrow(i), \quad i \in \mathbb{N}_0. \quad (2.5)$$

Отсюда, пользуясь обозначениями (2.2), находим

$$\vec{v}(i + mn) = f_{mn-1}\vec{v}(i + mn - 1) + \dots + f_0\vec{v}(i), \quad i \in \mathbb{N}_0, \quad (2.6)$$

$$v(i + mn) = f_{mn-1}v(i + mn - 1) + \dots + f_0v(i), \quad i \in \mathbb{N}_0, \quad (2.7)$$

т. е. $v \in L_S(F)$. Известно (см., например, [1, 29]), что $T(v)|T(F) \leq \tau$. Предложение 1 доказано.

2.2. Доказательство теоремы 3

Лемма 12. Пусть $\Psi(x), \Phi(x) \in \check{S}[x]$ — унитарные многочлены. Тогда условие $L_S(\Phi) \subseteq L_S(\Psi)$ выполняется, если и только если $\Phi(x)$ делит $\Psi(x)$ справа.

Доказательство леммы 12. Достаточность следует из того, что множество $L_S(\Phi)$ есть левый $\check{S}[x]$ -модуль. Докажем необходимость. Разделим многочлен $\Psi(x)$ на многочлен $\Phi(x)$ с остатком справа в кольце $\check{S}[x]$:

$$\Psi(x) = H(x)\Phi(x) + G(x), \quad \deg G(x) < \deg \Phi(x). \quad (2.8)$$

Для доказательства леммы достаточно показать, что $G(x) = 0$. Умножая обе части соотношения (2.8) на произвольную последовательность $u \in L_S(\Phi)$, с учетом условия $L_S(\Phi) \subseteq L_S(\Psi)$ находим $G(x)u = 0$. Пусть многочлен $G(x)$ имеет вид

$$G(x) = \sum_{j \geq 0} G_j x^j, \quad G_j \in \check{S}.$$

Поочередно рассматривая в качестве ЛРП $u \in L_S(\Psi)$ все последовательности с начальными векторами вида $(0, 0, \dots, 0, a)$, находим $G_0(a) = 0$ для всех $a \in S$. Следовательно, $G_0 = 0$. Далее, рассматривая в качестве ЛРП $u \in L_S(\Psi)$ последовательности с начальными векторами $(0, 0, \dots, 0, a, 0)$, находим, что $G_1(a) = 0$ для всех $a \in S$. Отсюда следует, что $G_1 = 0$. Аналогично устанавливаем, что все коэффициенты многочлена $G(x)$ равны нулю. Лемма 12 доказана.

Лемма 13. Если $\Psi(x) \in \check{S}[x]$ — унитарный многочлен степени m , то существует такой унитарный многочлен $F_\Psi(x) \in R[x]$ степени mn , что для некоторого многочлена $\Phi(x) \in \check{S}[x]$ выполняются равенства

$$F_\Psi(x) = \Phi(x) \cdot \Psi(x) = \Psi(x) \cdot \Phi(x), \quad (2.9)$$

при этом

- 1) если $\Psi(x)$ — МП-многочлен, то многочлен $F_\Psi(x)$, обладающий свойством (2.9), определен однозначно,
- 2) $\Psi(x)$ есть МП-многочлен над $\check{S}$, если и только если $F_\Psi(x)$ есть МП-многочлен над R .

Доказательство леммы 13. Выберем в качестве $F_\Psi(x)$ характеристический многочлен матрицы A_Ψ вида (2.3). Тогда, как показано в доказательстве предложения 1,

$$L_S(\Psi) \subset L_S(F_\Psi).$$

Из леммы 12 следует, что найдется такой многочлен $\Phi_1(x) \in \check{S}[x]$, что

$$F_\Psi(x) = \Phi_1(x)\Psi(x). \quad (2.10)$$

Обозначим через E_{mn} единичную $mn \times mn$ -матрицу над R . Тогда

$$F_\Psi(x) = \chi_{A_\Psi}(x) = |E_{mn} - A_\Psi|.$$

Пользуясь стандартными свойствами определителей матриц над коммутативным кольцом (см., например, [27]), с учетом равенства (2.3) находим

$$\begin{aligned} F_\Psi(x) &= |Ex^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0| \\ &= |Ex^m - A_{m-1}^T x^{m-1} - \dots - A_1^T x - A_0^T| = \chi_{A_{\Psi^T}}(x). \end{aligned}$$

Следовательно, $L_S(\Psi^T) \subset L_S(F_\Psi)$, и по лемме 12 найдется такой многочлен $\Phi_2(x) \in \check{S}[x]$, что

$$F_\Psi(x) = \Phi_2(x)\Psi^T(x). \quad (2.11)$$

Пусть $\mathfrak{M} : R_{n,n}[x] \rightarrow R[x]_{n,n}$ — канонический изоморфизм колец [27]. Рассматривая равенство (2.11) как равенство над кольцом $R_{n,n}[x]$ и применяя к обеим его частям изоморфизм $\mathfrak{M}$, получаем

$$\mathfrak{M}(F_\Psi) = \mathfrak{M}(\Phi_2)\mathfrak{M}(\Psi^T). \quad (2.12)$$

Заметим, что образ $\mathfrak{M}(F_\Psi)$ многочлена $F_\Psi(x)$ есть многочлен над $R_{n,n}$, все коэффициенты которого являются диагональными матрицами в силу условия $F_\Psi(x) \in R[x]$. Следовательно, имеет место равенство

$$\mathfrak{M}(F_\Psi)^T = \mathfrak{M}(F_\Psi).$$

С учетом (2.12) получаем

$$\mathfrak{M}(F_\Psi) = \mathfrak{M}(F_\Psi)^T = \mathfrak{M}(\Psi^T)^T \mathfrak{M}(\Phi_2)^T.$$

Применяя обратный изоморфизм $\mathfrak{M}^{-1}$ к обеим частям последнего равенства, принимая во внимание соотношения

$$\mathfrak{M}(\Psi^T)^T = \mathfrak{M}(\Psi), \quad \mathfrak{M}(\Phi_2)^T = \mathfrak{M}(\Phi_2^T),$$

имеем

$$F_\Psi(x) = \Psi(x)\Phi_2^T(x). \quad (2.13)$$

Покажем, что

$$\Phi_1(x) = \Phi_2^T(x). \quad (2.14)$$

Умножив обе части равенства $\Phi_1(x)\Psi(x) = \Psi(x)\Phi_2^T(x)$ на $\Phi_2^T(x)$ справа, в силу условия $F_\Psi(x) \in R[x]$ получим

$$\Phi_1(x)F_\Psi(x) = F_\Psi(x)\Phi_2^T(x) = \Phi_2^T(x)F_\Psi(x).$$

Отсюда находим $(\Phi_1(x) - \Phi_2^T(x))F_\Psi(x) = 0$. Так как $F_\Psi(x)$ — унитарный многочлен, последнее равенство возможно только при $\Phi_1(x) = \Phi_2^T(x)$. Тем самым равенство (2.14) доказано. Теперь (2.9) следует из (2.10), (2.13), (2.14).

Докажем утверждение п. 1 леммы 13. Предположим противное. Пусть найдутся различные унитарные многочлены $F_1(x), F_2(x) \in R[x]$ степени mn , для которых

$$F_i(x) = \Phi_i(x)\Psi(x), \quad i \in \{1, 2\}.$$

Положим $H(x) = F_1(x) - F_2(x)$ и покажем, что $H(x) = 0$. Пусть $v \in L_S(\Psi)$ — произвольная скрученная МП ЛРП. Тогда имеют место равенства

$$F_i(x)v = (\Phi_i(x)\Psi(x))v = \Phi_i(x)(\Psi(x)v) = 0, \quad i \in \overline{1, 2}. \quad (2.15)$$

Напомним, что $\vec{\alpha} = (\alpha_1, \dots, \alpha_{n-1})$ — базис свободного модуля ${}_R S$. Последовательности v соответствует единственный набор $v_0, \dots, v_{n-1}$ ее *координатных* последовательностей над R , определяемых условием

$$v(i) = \alpha_0 v_0(i) + \alpha_1 v_1(i) + \dots + \alpha_{n-1} v_{n-1}(i), \quad i \geq 0. \quad (2.16)$$

В силу условия $F_i(x) \in R[x]$ с учетом (2.15) и (2.16) находим

$$F_i(x)v_j = 0, \quad j \in \overline{0, n-1}, \quad i \in \overline{1, 2}. \quad (2.17)$$

Согласно [3] существует такой МП-многочлен $G(x)$ над R степени mn , что все координатные последовательности $v_0, \dots, v_{n-1}$ суть классические МП ЛРП над R из семейства $L_R(G)$. Пусть $\text{Ann}_{R[x]} v_j$ — аннулятор над R последовательности v_j , где $j \in \overline{0, n-1}$, т. е. множество

таких многочленов $A(x) \in R[x]$, что $A(x)v_j = 0$. Известно (см., например, [31]), что

$$\text{Ann}_{R[x]}v_j = R[x]G(x), \quad j \in \overline{0, n-1}.$$

Из условия (2.17) получаем

$$0 = F_1(x)v_j - F_2(x)v_j = (F_1(x) - F_2(x))v_j = H(x)v_j, \quad j \in \overline{0, n-1}.$$

Заметим, что $\deg H(x) < mn$, так как $F_1(x)$ и $F_2(x)$ суть унитарные многочлены степени mn . Таким образом, унитарный многочлен $G(x)$ степени mn делит над кольцом R многочлен $H(x)$ меньшей степени. Последнее возможно тогда и только тогда, когда $H(x) = 0$. Противоречие. Следовательно, $F_1(x) = F_2(x)$.

Докажем утверждение п. 2 леммы 13. Пусть $\Psi(x)$ — МП-многочлен над $\tilde{S}$. Тогда существует такая последовательность $v \in L_S(\Psi)$, что $T(v) = \tau$. Далее, так как $F_\Psi(x) \in R[x]$, $\deg F_\Psi = mn$, то $T(F_\Psi) \leq \tau$ (см., например, [2]). С другой стороны,

$$v \in L_S(\Psi) \subset L_S(F_\Psi),$$

следовательно, $\tau = T(v) \leq T(F_\Psi) \leq \tau$. Таким образом, $T(F_\Psi) = \tau$.

Обратно, предположим, что $F_\Psi(x)$ — МП-многочлен, и покажем, что $\Psi(x)$ также является МП-многочленом. Пусть $K = \text{GR}(q^{mnd}, p^d)$ — расширение Галуа степени m кольца S , а $\varkappa$ — автоморфизм Фробениуса кольца K над R (см., например, [2]). Согласно [2] многочлен $F_\Psi(x)$ имеет следующее разложение над K :

$$F_\Psi(x) = \prod_{j=0}^{mn-1} (x - \varkappa^j(\vartheta)), \quad (2.18)$$

при этом порядок $\text{ord } \vartheta$ элемента ϑ в мультипликативной группе кольца K равен τ . Согласно [2] каждая ЛРП $v \in L_K(F_\Psi)$ представляется в виде суммы биномиальных последовательностей с различными корнями, имеющими порядок τ . Так как $\Psi(x)$ делит $F_\Psi(x)$ справа, то по лемме 12

$$L_S(\Psi) \subset L_S(F_\Psi) \subset L_K(F_\Psi).$$

Таким образом, любая ЛРП $v \in L_S(\Psi) \subset L_K(F_\Psi)$, удовлетворяющая условию $\|v\| = \max\{j \in \overline{0, d-1} : v \in p^j S^{(1)}\} = 0$, имеет период τ (см., например, [2]). Следовательно, $\Psi(x)$ — МП-многочлен.

Лемма 13 доказана.

Перейдем к *доказательству* теоремы 3. Для краткости будем обозначать тот факт, что из п. i теоремы 3 следует п. j , следующим образом: $(i) \Rightarrow (j)$, где $i, j \in \overline{1, 4}$. Равносильность $(1) \Leftrightarrow (2)$ следует из леммы 13. Из леммы 13 следуют также импликации $(1) \Rightarrow (3)$ и $(1) \Rightarrow (4)$. Для доказательства импликации $(3) \Rightarrow (1)$ заметим, что по лемме 12 из равенства $F = \Phi(x)\Psi(x)$ для некоторого многочлена $\Phi(x) \in R[x]$ следует соотношение $L_S(\Psi) \subset L_S(F)$. Следовательно, как отмечено в доказательстве п. 2 леммы 13, любая последовательность $v \in L_S(\Psi)$ с $\|v\| = 0$ имеет период τ . Таким образом, $\Psi(x)$ — МП-многочлен. Тем самым импликация $(3) \Rightarrow (1)$ установлена.

Докажем импликацию $(4) \Rightarrow (1)$. По условию существует такой многочлен $\Phi(x) \in \check{S}[x]$, что $F(x) = \Psi(x)\Phi(x)$. Тогда

$$F(x) = F^T(x) = \Phi^T(x)\Psi^T(x).$$

В силу доказанной равносильности п. 1 и п. 3 теоремы 3 многочлен $\Psi^T(x)$ является МП-многочленом, при этом $\Psi^T(x) \in \text{MP}(F)$. Тогда, как показано в доказательстве п. 2 леммы 13,

$$\Psi(x) = (\Psi^T(x))^T \in \text{MP}(F).$$

Следовательно, существует такой многочлен $\Phi_1(x)$, что $F(x) = \Phi_1(x)\Psi(x)$. В силу доказанной импликации $(3) \Rightarrow (1)$ многочлен $\Psi(x)$ есть МП-многочлен над $\check{S}$. Теорема 3 доказана.

2.3. Доказательство теоремы 6

Пусть $\Psi(x) \in \text{MP}(F)$; тогда существует такой многочлен $\Phi(x) \in \check{S}[x]$, что $F(x) = \Phi(x)\Psi(x)$. Учитывая условие $F(x) \in R[x]$, находим:

$$F^{(A)}(x) = F(x) = \Phi^{(A)}(x)\Psi^{(A)}(x).$$

Следовательно, если $\Psi^{(A)}(x)$ есть унитарный многочлен степени m , то по теореме 3 справедливо включение $\Psi^{(A)}(x) \in \text{MP}(F)$.

Обратно. Пусть $\Psi^{(A)}(x)$ — МП-многочлен над $\check{S}$; покажем, что его степень равна m . Если $\Psi^{(A)}(x)$ унитарный и его степень больше m , то он не является МП-многочленом, так как для произвольной последовательности $v \in L_S(\Psi^{(A)}) \subset L_S(F)$ выполняется условие

$$T(v) \leq T(F) = \tau < (q^{n \cdot \deg \Psi^{(A)}} - 1)p^{d-1}.$$

Покажем, что случай, когда $\Psi^{(A)}$ — унитарный многочлен степени $m' < m$, невозможен. Предположим противное: пусть $\deg \Psi^{(A)}(x) =$

$m' < m$. Покажем, что $m' \neq 0$. Действительно, из условия $\Psi^{(A)}(x) = e$ следует, что $\Psi(x) = e$, т. е. $m = 0$. Однако $m \geq 1$.

Таким образом, справедливо неравенство $m' \geq 1$. По лемме 13 существует такой унитарный многочлен $F_1(x) \in R[x]$ степени $m'n$, что $F_1(x) = \Phi_1(x)\Psi^{(A)}(x)$ для некоторого $\Phi_1(x) \in \check{S}[x]$. Так как $F(x)$ — МП-многочлен, то из условия $\deg F(x) > \deg F_1(x)$ следует, что многочлены $F(x)$ и $F_1(x)$ взаимно просты [2]. Поэтому существуют такие многочлены $U(x), V(x) \in R[x]$, что

$$U(x)F(x) + V(x)F_1(x) = (U(x)\Phi(x) + V(x)\Phi_1(x))\Psi^{(A)}(x) = e.$$

Последнее равенство невозможно, так как $\Psi^{(A)}(x)$ есть унитарный многочлен ненулевой степени.

2.4. Доказательство предложения 7

Заметим, что так как кольцо R есть центр кольца $\check{S}$, то имеет место равенство

$$\Psi^{(A)}(x) = x^m - \sum_{j=t+1}^{m-1} \psi_j x^j - \sum_{j=0}^t A^{-1}(x) \psi_j A(x) x^j.$$

Следовательно, при выполнении условий п. 1 предложения 7

$$\deg \Psi^{(A)}(x) = m,$$

по теореме 6 многочлен $\Psi^{(A)}(x)$ является МП-многочленом над $\check{S}$.

Рассмотрим случай, когда R — поле и $n = 2$. Используя изоморфизм колец $\check{S}[x]$ и $R_{n,n}[x]$ и вычисляя обратный многочлен $A^{-1}(x)$ как матрицу, обратную к $A(x)$, находим, что $\deg A(x) = \deg A^{-1}(x)$. Теперь справедливость п. 2 предложения 7 следует из п. 1 предложения 7.

2.5. Доказательство предложения 8

В доказательстве п. 2 леммы 13 установлено соотношение

$$L_S(\Psi) \subset L_S(F) \Leftrightarrow L_S(\Psi^T) \subset L_S(F).$$

Отсюда с учетом п. 2 леммы 13 следует справедливость предложения 8.

2.6. Доказательство предложения 9

Далее для элемента t произвольного кольца P и эндоморфизма $g \in \text{End}(P)$ через t^g будем обозначать образ $g(t)$ элемента t под действием g .

Лемма 14. Пусть P — произвольное коммутативное кольцо, G — конечная абелева подгруппа мультипликативной группы кольца $\text{End}(P)$ и $P^{(G)}$ — скрученное групповое кольцо группы G над кольцом P . Тогда отображение $\nu : P^{(G)} \rightarrow P^{(G)}$, заданное по правилу

$$\nu \left(\sum_{g \in G} p_g g \right) = \sum_{g \in G} p_g^{g^{-1}} g^{-1} = \sum_{g \in G} p_{g^{-1}}^g g, \quad (2.19)$$

есть инволюция кольца $P^{(G)}$.

Доказательство леммы 14. Пусть $\beta = \sum_{g \in G} p_g g, \gamma = \sum_{g \in G} t_g g \in P^{(G)}$.

Докажем, что

$$\nu(\beta \cdot \gamma) = \nu(\gamma)\nu(\beta). \quad (2.20)$$

Имеем

$$\beta \cdot \gamma = \left(\sum_{g \in G} p_g g \right) \left(\sum_{g \in G} t_g g \right) = \sum_{f \in G} \left(\sum_{g, h \in G, g \cdot h = f} p_g t_h^g \right) f.$$

Следовательно,

$$\nu(\beta \cdot \gamma) = \sum_{f \in G} \left(\sum_{g, h \in G, g \cdot h = f^{-1}} p_g^f t_h^{gf} \right) f. \quad (2.21)$$

С другой стороны,

$$\nu(\gamma) \cdot \nu(\beta) = \left(\sum_{h \in G} t_{h^{-1}}^h h \right) \cdot \left(\sum_{g \in G} p_{g^{-1}}^g g \right) = \sum_{f \in G} \left(\sum_{h, g \in G, h \cdot g = f} t_{h^{-1}}^h p_{g^{-1}}^{gh} \right) f. \quad (2.22)$$

С учетом коммутативности группы G находим

$$\sum_{h, g \in G, h \cdot g = f} t_{h^{-1}}^h p_{g^{-1}}^{gh} = \sum_{h, g \in G, g \cdot h = f} t_{h^{-1}}^{g^{-1}f} p_{g^{-1}}^f = \sum_{h, g \in G, g^{-1} \cdot h^{-1} = f^{-1}} t_{h^{-1}}^{g^{-1}f} p_{g^{-1}}^f.$$

Далее,

$$\sum_{h,g \in G, g^{-1} \cdot h^{-1} = f^{-1}} t_{h^{-1}}^{g^{-1}f} p_{g^{-1}}^f = \sum_{h^{-1}, g^{-1} \in G, g^{-1} \cdot h^{-1} = f^{-1}} t_{h^{-1}}^{g^{-1}f} p_{g^{-1}}^f = \sum_{h,g \in G, g \cdot h = f^{-1}} t_h^{gf} p_g^f.$$

В силу коммутативности кольца P

$$\sum_{h,g \in G, g \cdot h = f^{-1}} t_h^{gf} p_g^f = \sum_{h,g \in G, g \cdot h = f^{-1}} p_g^f t_h^{gf}. \quad (2.23)$$

Теперь (2.20) следует из соотношений (2.21), (2.22), (2.23). Условия

$$\nu(\beta + \gamma) = \nu(\beta) + \nu(\gamma), \nu(\nu(\beta)) = \beta$$

напрямую следуют из (2.19). Лемма 14 доказана.

По лемме 14 соответствие $\phi \rightarrow \phi^{[*]}$ есть инволюция кольца $\check{S}$. Несложно проверить, что из равенства $(\phi \cdot \psi)^{[*]} = \psi^{[*]} \cdot \phi^{[*]}$ для всех $\phi, \psi \in \check{S}$ следует равенство $(\Phi(x)\Psi(x))^{[*]} = \Psi^{[*]}(x) \cdot \Phi^{[*]}(x)$ для всех $\Phi(x), \Psi(x) \in \check{S}[x]$.

Если $\Psi(x) \in \text{MP}(F)$, то существует такой многочлен $\Phi(x) \in \check{S}[x]$, что

$$F(x) = \Phi(x)\Psi(x). \quad (2.24)$$

Последнее выполнено тогда и только тогда, когда

$$F(x) = F^{[*]}(x) = \Psi^{[*]}(x)\Phi^{[*]}(x).$$

Таким образом, в силу равносильности п. 1 и п. 4 теоремы 3 многочлен $\Psi^{[*]}(x)$ является МП-многочленом из семейства $\text{MP}(F)$. Предложение 9 доказано.

2.7. Доказательство предложения 10

Непосредственной проверкой доказывается следующее утверждение.

Лемма 15. Если $A(x) = \sum_{j \geq 0} a_j x^j, B(x) = \sum_{k \geq 0} b_k x^k \in \check{S}[x]$ — реверсивные многочлены, то

$$\begin{aligned} A(x)^{**} &= A(x), \quad A(x)^{(*)^{(*)}} = A(x), \\ (A(x) \cdot B(x))^* &= b_0^{-1} A^*(x) b_0 \cdot B^*(x), \\ (A(x) \cdot B(x))^{(*)} &= A^{(*)}(x) \cdot a_0 B^{(*)}(x) a_0^{-1}. \end{aligned}$$

Если $\Psi(x) \in \text{MP}(F)$, то существует такой многочлен $\Phi(x) \in \check{S}[x]$, что выполнено равенство (2.24). Так как $F(x)$ — реверсивный многочлен, то $\Psi(x)$ также есть реверсивный многочлен. По лемме 15 равенство (2.24) эквивалентно равенству $F^*(x) = \psi_0^{-1} \Phi^*(x) \psi_0 \cdot \Psi^*(x)$. Покажем, что $F^*(x)$ — МП-многочлен. Для этого достаточно доказать, что корень многочлена $F^*(x)$ в расширении $K = \text{GR}(q^{nmd}, p^d)$ кольца R есть элемент порядка τ . Пусть ϑ — корень $F(x)$ в K . Так как $F(x)$ — МП-многочлен, то $\text{ord } \vartheta = \tau$. Несложно видеть, что ϑ^{-1} — корень $F^*(x)$ в K . Для завершения доказательства п. 1 осталось воспользоваться равенством $\text{ord } \vartheta = \text{ord } \vartheta^{-1}$.

Докажем п. 2. Если $\Psi(x) \in \text{MP}(F)$, то по теореме 3 найдется такой многочлен $\Phi(x)$ над $\check{S}$, что $F(x) = \Phi(x)\Psi(x) = \Psi(x)\Phi(x)$. С использованием леммы 15 получаем

$$F^{(*)}(x) = \Psi^{(*)}(x) \psi_0 \Phi^{(*)}(x) \psi_0^{-1}.$$

Из теоремы 3 следует что $\Psi^{(*)}(x)$ есть МП-многочлен из семейства $\text{MP}(F^{(*)})$. Для завершения доказательства осталось заметить, что $F^{(*)}(x) = F^*(x)$ есть МП-многочлен над R . Предложение 10 доказано.

2.8. Доказательство теоремы 11

Отметим, что так как $\Psi(x)$ является реверсивным многочленом и многочлены $h(x)$ и $g(x)$ суть ненулевые многочлены над полем, то свободный член многочлена (1.21) обратим, и многочлен (1.22) определен корректно.

Так как $\Psi(x)$ — МП-многочлен из семейства $\text{MP}(F)$, то в кольце $\check{S}[x]$ имеет место равенство

$$F(x) = \Phi(x)\Psi(x). \quad (2.25)$$

С другой стороны, $F(x)$ имеет следующее каноническое разложение над полем K :

$$F(x) = (x - \vartheta)(x - \varkappa(\vartheta)) \cdot \dots \cdot (x - \varkappa^{mn-1}(\vartheta)),$$

где $\varkappa$ — произвольный автоморфизм Фробениуса K над R (см., например, [2]). Отметим, что в случае когда R — поле, последнее разложение имеет вид

$$F(x) = (x - \vartheta)(x - \vartheta^q) \cdot \dots \cdot (x - \vartheta^{q^{mn-1}}). \quad (2.26)$$

Без ограничения общности можем считать, что действие автоморфизма $\varkappa$ поля K над R на элементе $\eta \in K$ определено равенством $\varkappa(\eta) = \eta^{|R|} = \eta^q$ и что автоморфизм σ поля S над R есть ограничение $\varkappa$ на S , т. е. выполнено равенство

$$\varkappa|_S = \sigma.$$

Скрученное групповое кольцо $\check{K} = K^{\varkappa}\langle \varkappa \rangle$ содержит в себе подкольцо

$$\tilde{S} = \left\{ \sum_{j=0}^{n-1} s_j \varkappa^j | s_j \in S, j \in \overline{0, n-1} \right\} \subset \check{K},$$

при этом соответствие

$$\xi : \check{S} \rightarrow \tilde{S}, \quad \xi \left(\sum_{j=0}^{n-1} s_j \sigma^j \right) = \sum_{j=0}^{n-1} s_j \varkappa^j$$

задает изоморфизм колец $\check{S}$ и $\tilde{S}$. Изоморфизм ξ продолжается до автоморфизма Ξ колец многочленов $\check{S}[x]$ и $\tilde{S}[x]$ естественным образом по правилу

$$\Xi \left(\sum_{j \geq 0} a_j x^j \right) = \sum_{j \geq 0} \xi(a_j) x^j.$$

Пусть $\Phi_1(x) = \Xi(\Phi(x)) = \sum_{j \geq 0} \phi_j^{(1)} x^j$ и $\Psi_1(x) = \Xi(\Psi(x)) = \sum_{j \geq 0} \psi_j^{(1)} x^j$. Применяя изоморфизм Ξ к обеим частям равенства (2.25), с учетом (2.26) приходим к следующему равенству над $\check{K}[x]$:

$$(x - \vartheta)(x - \vartheta^q) \cdot \dots \cdot (x - \vartheta^{q^{mn-1}}) = \Phi_1(x) \cdot \Psi_1(x). \quad (2.27)$$

Рассмотрим отображение Υ кольца $\check{K}[x]$ в кольцо $\check{K}[x, y]$, действующее по правилу

$$\Upsilon \left(\sum_{j=0}^t a_j x^j \right) = \sum_{j=0}^t a_j x^j y^{t-j}.$$

Несложно видеть, что Υ есть гомоморфизм колец. Применяя гомоморфизм Υ к обеим частям равенства (2.27), находим

$$\prod_{j=0}^{mn-1} (x - \vartheta^{q^j} y) = \sum_{j=0}^{m(n-1)} \phi_j^{(1)} x^j y^{m(n-1)-j} \cdot \sum_{j=0}^m \psi_j^{(1)} x^j y^{m-j}. \quad (2.28)$$

Напомним, что многочлены $h(x), g(x)$ принадлежат кольцу $R[x]$, которое содержится в центре кольца $\check{K}[x, y]$. Учитывая данное обстоятельство и вычисляя значения многочленов из левой и правой частей

равенства (2.28) в точке $(h(x), g(x))$, получаем

$$\prod_{j=0}^{mn-1} (h(x) - \vartheta^{q^j} g(x)) = \sum_{j=0}^{m(n-1)} \phi_j^{(1)} h(x)^j g(x)^{m(n-1)-j} \cdot \sum_{j=0}^m \psi_j^{(1)} h(x)^j g(x)^{m-j}. \quad (2.29)$$

Пусть

$$G(x) = \prod_{j=0}^{mn-1} (h(x) - \vartheta^{q^j} g(x)) \in K[x]. \quad (2.30)$$

Продолжим автоморфизм $\mathfrak{K}$ поля K над R до автоморфизма $\hat{\mathfrak{K}}$ кольца $K[x]$ естественным образом (по аналогии с продолжением ξ до Ξ). Из [30] известно, что произвольный многочлен $f(x) \in K[x]$ есть многочлен из $R[x]$ тогда и только тогда, когда $\hat{\mathfrak{K}}(f(x)) = f(x)$. В силу равенства $\hat{\mathfrak{K}}(G(x)) = G(x)$ справедливо включение

$$G(x) \in R[x]. \quad (2.31)$$

Пусть $\Phi_2(x) = \Xi^{-1} \left(\sum_{j=0}^{m(n-1)} \phi_j^{(1)} h(x)^j g(x)^{m(n-1)-j} \right)$. Напомним, что

$\Lambda(x)$ есть многочлен (1.21). Применяя автоморфизм Ξ^{-1} к обеим частям равенства (2.29), в силу условий (2.30), (2.31) находим

$$G(x) = \Phi_2(x) \Lambda(x) = \Phi_2(x) (\lambda_{mk}^{-1} \Lambda(x)). \quad (2.32)$$

Таким образом, унитарный многочлен $(\lambda_{mk}^{-1} \Lambda(x))$ над $\check{S}$ степени mk делит справа унитарный многочлен $G(x)$ над R степени mn . Из теоремы 3 следует, что $(\lambda_{mk}^{-1} \Lambda(x))$ есть МП-многочлен над $\check{S}$, если и только если $G(x)$ есть МП-многочлен над R , т. е. если некоторый корень многочлена $G(x)$ в расширении $K_1 = \text{GF}(q^{mnk})$ поля K является примитивным элементом. Пусть θ — корень многочлена $G(x)$ в K_1 . В силу разложения (2.30) найдется такое $j \in \overline{0, mn-1}$, что θ — корень многочлена $h(x) - \vartheta^{q^j} g(x)$ степени k над K . Следовательно, примитивный элемент $\theta^{q^{mn-j}}$ поля K_1 является корнем многочлена $h(x) - \vartheta g(x)$. Таким образом, $h(x) - \vartheta g(x)$ есть МП-многочлен над K . Теорема 11 доказана.

Автор выражает признательность О.А. Козлитину, внимательно прочитавшему рукопись и сделавшему ряд ценных замечаний.

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] Zaitsev 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., 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** (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] Lam T.Y., *A First Course in Noncommutative Rings*, New York: Springer–Verlag, 1991.
- [27] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра*. Т. 2, М.: Гелиос АРВ, 2003.
- [28] Ленг С., *Алгебра*, М.: Мир, 1968.
- [29] Нечаев А.А., “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сб.*, **184**:3 (1993), 21–56.
- [30] Лидл Р., Нидеррайтер Г., *Конечные поля*, М.: Мир, 1988.
- [31] Нечаев А.А., “Линейные рекуррентные последовательности над коммутативными кольцами”, *Дискретная математика*, **3**:4 (1991), 105–127.