М. А. Гольтваница, Представления скрученных линейных рекуррентных последовательностей максимального периода над конечным полем, *Матем. вопр. криптогр.*, 2023, том 14, выпуск 1, 27–43

DOI: 10.4213/mvk429

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2023 Т. 14 № 1 С. 27–43

УДК 519.113.6+519.719.2 DOI https://doi.org/10.4213/mvk429

Представления скрученных линейных рекуррентных последовательностей максимального периода над конечным полем

М. А. Гольтваница

ООО «Центр сертификационных исследований», Москва

Получено 27.V.2022

Аннотация. Пусть p — простое число, $R = \mathrm{GF}(q)$ — поле из q элементов, где $q = p^r$, $S = \mathrm{GF}(q^n)$ — его расширение степени n и $\check{S}$ — кольцо линейных преобразований векторного пространства ${}_RS$. Последовательность v над S, удовлетворяющую закону рекурсии

$$\forall i \in \mathbb{N}_0 \colon v(i+m) = \psi_{m-1}(v(i+m-1)) + \ldots + \psi_0(v(i)), \psi_0, \ldots, \psi_{m-1} \in \check{S},$$

будем называть *скрученной линейной рекуррентной последовательностью* над S порядка m с характеристическим многочленом $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$. Максимально возможный период последовательности такого вида равен $q^{mn} - 1$. Пусть v — скрученная ЛРП максимального периода над S. Далее для произвольного кольца J с единицей $\mathbf{e}$, для которого элемент $q\mathbf{e}$ не является делителем нуля, и отображения $f : S \to J$ при некоторых условиях описан аннулятор последовательности $f(v)$.

Ключевые слова: конечное поле, последовательность максимального периода, скрученная ЛРП, ранг, аннулятор

Representations of skew linear recurrent sequences of maximal period over finite field

M. A. Goltvanitsa

LLC «Certification Research Center», Moscow

Abstract. Let p be a prime number, $R = \mathrm{GF}(q)$ be a finite field, where $q = p^r$, $S = \mathrm{GF}(q^n)$ be its extension of degree n and $\check{S}$ be a ring of linear transforms of the vector space ${}_RS$. A sequence v over S with a recursion law of the form

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

Citation: Matematicheskie Voprosy Kriptografii, 2023, v. 14, № 1, pp. 27–43 (Russian)

is called *skew linear recurrent sequence* over S of order m with the characteristic polynomial $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$. It is well known that maximal period of such sequence is equal to $q^{mn} - 1$. Let v be a skew LRS of maximal period over S, J be an arbitrary ring with identity $\mathbf{e}$ such that $q\mathbf{e}$ is not a zero divisor and $f : S \to J$ be a map. Below under certain conditions we describe the annihilator of the sequence $f(v)$.

Keywords: finite field, ML-sequence, skew LRS, rank, annihilator

1. Введение. Основные результаты

Далее $R = \mathrm{GF}(q)$ — поле из q элементов, $q = p^r$, p — простое число, $S = \mathrm{GF}(q^n)$ — его расширение степени n. Известно, что группа $\mathrm{Aut}(S/R)$ автоморфизмов S над R есть циклическая группа порядка n [1]. Пусть σ — образующий элемент данной группы, $\check{S} = S^\sigma\langle\sigma\rangle$ — скрученное групповое кольцо группы $\langle\sigma\rangle$ над S, т. е. кольцо $\check{S}$ есть множество всевозможных формальных сумм вида

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

с естественным сложением и умножением, определяемым по дистрибутивности из тождества

$$\forall s \in S: \quad \sigma s = \sigma(s)\sigma. \tag{1.1}$$

Каждый элемент $\psi \in \check{S}$ задает линейное преобразование векторного пространства ${}_RS$, действие которого на элементе $s \in S$ определяется равенством

$$\psi(s) = \sum_{j=0}^{n-1} s_j\sigma^j(s), \tag{1.2}$$

и, обратно, каждое линейное преобразование пространства ${}_RS$ имеет такой вид. Поэтому справедливы изоморфизмы

$$\check{S} \cong \mathrm{End}({}_RS) \cong R_{n,n}, \tag{1.3}$$

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

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

Следуя [2], последовательность $v \in S^{\langle 1\rangle}$ назовем *скрученной линейной рекуррентной последовательностью* (*ЛРП*) порядка $m > 0$ над кольцом S, если v есть ЛРП порядка m над модулем ${}_{\check{S}}S$ [3,4]. Иначе говоря, если справедливо равенство $\Psi(x)v = 0$ для некоторого унитарного многочлена

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \ldots - \psi_0 \in \check{S}[x] \tag{1.4}$$

степени m, называемого *характеристическим многочленом ЛРП* v, т. е. если последовательность v удовлетворяет закону рекурсии

$$\forall i \in \mathbb{N}_0: \quad v(i+m) = \psi_{m-1}(v(i+m-1)) + \ldots + \psi_0(v(i)). \tag{1.5}$$

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*.

Несложно видеть, что если v — скрученная ЛРП порядка m над S, то для периода $T(v)$ последовательности v имеет место оценка

$$T(v) \leqslant \mathbf{T} = q^{nm} - 1.$$

Если выполнено равенство

$$T(v) = \mathbf{T},$$

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.

Зафиксируем базис $\vec{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ пространства ${}_RS$ и обозначим через $a^{\downarrow} = (a_0, \ldots, a_{n-1})^T \in R^{(n)}$ 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 $\psi \in \check{S}$ пространства ${}_RS$ 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 $v \in S^{\langle 1\rangle}$ является скрученной ЛРП порядка m, т. е. удовлетворяет соотношению вида (1.5), тогда и только тогда, когда столбцы координат $v^{\downarrow}(i)$ членов этой последовательности в базисе $\vec{\alpha}$ удовлетворяют соотношению

$$\forall i \in \mathbb{N}_0 : v^{\downarrow}(i+m) = A(\psi_{m-1})v^{\downarrow}(i+m-1) + \ldots + A(\psi_0)v^{\downarrow}(i). \quad (1.6)$$

Всюду далее для неотрицательных целых чисел a, b, $a \leqslant b$, через $\overline{a,b}$ обозначаем множество $\{a, a+1, \ldots, b\}$. Согласно (1.3) матрицы $A_s = A(\psi_s) \in R_{n,n},\ s \in \overline{0, m-1}$, в (1.6) могут быть произвольными, и закон рекурсии (1.6) можно записать компактнее:

$$v^{\downarrow}(i+m) = A_{m-1}v^{\downarrow}(i+m-1) + \ldots + A_0v^{\downarrow}(i), A_0, \ldots, A_{m-1} \in R_{n,n}, i \geqslant 0. \quad (1.7)$$

Именно такие последовательности изучались ранее в статьях [5–11].

Далее приводим краткий обзор предшествующих результатов и фактов о скрученных ЛРП, необходимых для дальнейшего изложения.

Интерес к множеству скрученных ЛРП с точки зрения криптографии обусловлен прежде всего тем, что оно включает в себя классические ЛРП и значительно превосходит множество классических ЛРП по мощности [12]. Данное обстоятельство приводит к тому, что порой удается построить скрученные МП ЛРП, обладающие конструктивными преимуществами по сравнению с классическими ЛРП и подходящие для программной реализации [13–15].

Систематическое изучение свойств скрученных МП ЛРП над произвольными кольцами Галуа было начато в [2], 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. Далее через $\check{S}^*$ обозначаем мультипликативную группу кольца $\check{S}$.

Теорема 1 ([2]). *Пусть* v *— скрученная МП ЛРП порядка* m *над* S *с характеристическим многочленом* $\Psi(x) = x^m - \sum_{i=0}^{m-1} \psi_i x^i \in \check{S}[x]$, $\psi \in \check{S}$, *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* m *над* S, *то* $\psi \in \check{S}^*$.

Если выполнены условия п. 1 теоремы 1, а v — классическая МП ЛРП порядка m 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 [2]. Множество линеаризуемых МП-многочленов полностью описано в [2], там же доказана формула для его мощности и вычислены ранги скрученных МП ЛРП с характеристическими многочленами из этого множества. Существенное продвижение в направлении построения скрученных МП ЛРП и МП-многочленов над $\check{S}$, основанное на идее факторизации многочленов в кольце $\check{S}[x]$, сделано в статье [16], где доказаны обобщения теоремы 1. Отметим, что задача описания всех нелинеаризуемых МП ЛРП и МП-многочленов не решена по сей день. Тем не менее в статьях [14–19] доказаны теоремы, позволяющие строить нелинеаризуемые скрученные МП ЛРП и МП-многочлены над $\check{S}$.

При заданном базисе $\vec{\alpha}$ пространства ${}_RS$ произвольной последовательности $v \in S^{\langle 1\rangle}$ соответствует единственный набор последовательностей

$$v_0, \ldots, v_{n-1} \in R^{\langle 1\rangle},$$

для которого

$$v = v_0\alpha_0 + v_1\alpha_1 + \ldots + v_{n-1}\alpha_{n-1}. \tag{1.8}$$

Будем называть $v_0, \ldots, v_{n-1}$ *координатными последовательностями* последовательности v (в базисе $\vec{\alpha}$). Отметим, что ранее в отечественной литературе (см., например, [20]) термин "координатные последовательности" использовался для последовательностей другого типа, которые в настоящее называются разрядными последовательностями.

В [2] получена следующая характеризация всех скрученных МП ЛРП.

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

$$\forall i \in \mathbb{N}_0 : (v(i), \ldots, v(i+m-1) \neq (0, \ldots, 0) \tag{1.9}$$

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* (1.8) *есть линейно независимая система МП ЛРП из* $L_R(F)$.

Отметим, что одной из важнейших алгебраических криптографических характеристик псевдослучайных последовательностей является ранг (линейная сложность). Обозначим через $\operatorname{rank}_S v$, $\operatorname{rank}_R v$ ранг (степень минимального многочлена) последовательности $v \in S^{\langle 1\rangle}$, рассматриваемой как ЛРП над векторными пространствами ${}_SS$ и ${}_RS$, соответственно (см. [3]).

Из теоремы 2 следует, что для любой скрученной МП ЛРП v над S выполняется равенство $\operatorname{rank}_R v = mn$. Если v — классическая МП ЛРП над S, то $\operatorname{rank}_S v = m$. В статье [2] доказано, что если v — скрученная МП ЛРП порядка m над S, то справедливы неравенства

$$m \leqslant \operatorname{rank}_S v \leqslant nm. \tag{1.10}$$

Методы построения скрученных МП ЛРП порядка m над S, имеющих максимальный ранг mn, изложены в [15, 17].

Данная статья посвящена изучению свойств некоторых усложнений скрученных МП ЛРП. Построение псевдослучайных последовательностей с гарантированными алгебраическими и статистическими свойствами является важным и актуальным направлением современной криптографии. Один из способов получения таких последовательностей базируется на идее применения усложнений различных типов к классическим МП ЛРП, которые, несмотря на приемлемые статистические свойства и большой период, имеют низкую линейную сложность (ранг). Как уже было отмечено выше, скрученные МП ЛРП имеют более высокий ранг по сравнению с классическими МП ЛРП того же порядка. В связи с этим предлагается подход к построению псевдослучайных последовательностей, основанный на применении стандартных методов усложнения не к классическим, а к скрученным МП ЛРП. Однако исследование свойств усложнений скрученных МП ЛРП сопряжено со многими трудностями, вызванными отсутствием развитого математического аппарата для ЛРП над модулем с некоммутативным кольцом коэффициентов.

В то же время, как показано в [21–23], в ряде случаев к скрученным МП ЛРП применимы методы усложнения, которые позволяют полу-

чать псевдослучайные последовательности, имеющие лучшие криптографические характеристики по сравнению с псевдослучайными последовательностями, полученными из классических МП ЛРП того же порядка. К настоящему времени имеется много отечественных и зарубежных статей [2, 4–11, 13–19, 21–28], посвященных изучению скрученных ЛРП и их усложнений. В [21,22] изучались усложнения скрученных МП ЛРП, базирующиеся на идее выделения разрядных последовательностей, а в [23] — усложнения, являющиеся результатом вычисления некоторой нелинейной функции от нескольких знаков скрученной МП ЛРП. В настоящей работе исследуются усложнения скрученных МП ЛРП, основанные на использовании нескольких алгебраических структур. Перейдем к основным результатам.

Далее v — скрученная МП ЛРП порядка m над S. Из результатов статьи [2] известно, что существуют примитивный элемент θ из расширения $K = \mathrm{GF}(q^{mn})$ поля S и единственный набор $(\zeta_0, \ldots, \zeta_{n-1}) \in K^n$ со свойством

$$v(i) = \alpha_0 \operatorname{tr}_R^K(\zeta_0\theta^i) + \alpha_1 \operatorname{tr}_R^K(\zeta_1\theta^i) + \ldots + \alpha_{n-1} \operatorname{tr}_R^K(\zeta_{n-1}\theta^i),\ i \geqslant 0, \quad (1.11)$$

где tr_R^K — функция след [1] из поля K в S, значение которой на элементе $\epsilon \in K$ определяется равенством

$$\operatorname{tr}_R^K(\varepsilon) = \varepsilon + \varepsilon^q + \varepsilon^{q^2} + \ldots + \varepsilon^{q^{nm-1}}.$$

При этом система

$$\vec{\zeta} = \left(\zeta_0, \zeta_1, \ldots, \zeta_{n-1}, \zeta_0\theta, \ldots, \zeta_{n-1}\theta, \ldots, \zeta_0\theta^{m-1}, \ldots, \zeta_{n-1}\theta^{m-1}\right) \quad (1.12)$$

есть базис пространства ${}_RK$.

Напомним, что $\mathbf{T} = q^{mn} - 1$, и введем дополнительные обозначения

$$\tau = \frac{\mathbf{T}}{q-1}, \quad \beta = \theta^{\frac{q^{mn}-1}{q^n-1}}, \quad \gamma = \theta^\tau. \quad (1.13)$$

Далее также будем рассматривать последовательность

$$w(i) = \gamma^i,\ i \geqslant 0. \quad (1.14)$$

Отметим, что β — примитивный элемент поля S, а γ — примитивный элемент поля R. Введем обозначения

$$M_k^s(v) = \{i \in \overline{0, \mathbf{T}-1} \colon v(i+k) = s\},\ k \in \mathbb{N}_0,\ s \in S,$$

$$M_{k_1k_2}^{s_1s_2}(v) = \{i \in \overline{0, \mathbf{T}-1}\colon\ v(i+k_1) = s_1,\ v(i+k_2) = s_2\},\ k_1, k_2 \in \mathbb{N}_0,\ s_1, s_2 \in S.$$

Далее для упрощения формул иногда будем писать $M_{k_1k_2}^{s_1s_2}$ вместо $M_{k_1k_2}^{s_1s_2}(v)$ и M_k^s вместо $M_k^s(v)$, если ясно о какой последовательности v идет речь.

Пусть J — некоторое кольцо. Последовательность $f(v)$ над J, определяемую соотношениями

$$f(v)(i) = f(v(i)),\ i \geqslant 0,$$

назовем представлением последовательности v над кольцом J. Далее для множества многочленов $I \subset J[x]$ через (I) обозначим идеал в $J[x]$, порожденный множеством I.

При некоторых условиях удается установить связь между аннулятором последовательности $f(v)$ и аннулятором последовательности $f(w)$.

Теорема 3. *Пусть v — скрученная МП ЛРП порядка m над S, для которой справедливо разложение* (1.11), *имеют место равенства* (1.13), (1.14) *и J — такое коммутативное кольцо с единицей $\mathbf{e}$, что элемент $q\mathbf{e}$ не является делителем нуля. Пусть $f : S \to J$ — отображение, удовлетворяющее условию*

$$\forall \mu \in S \setminus R\colon\ f(\mu) = 0,\ f(0) = 0. \tag{1.15}$$

Тогда если существует такой многочлен $F(x) \in \mathrm{Ann}(f(w))$, что многочлены $F(x)$ и $x - \mathbf{e}$ взаимно просты, и если для всех $l \in \overline{0, q-2}$, $k \in \overline{1, \tau - 1}$

$$|M_{0k}^{e\gamma^l}(v)| = |M_{0k}^{\gamma\gamma^l}(v)|, \tag{1.16}$$

то

$$\mathrm{Ann} f(v) = (G(x^\tau) | G(x) \in \mathrm{Ann}(f(w))).$$

В основе теоремы 3 лежат результаты статьи [29], описывающие аннулятор представления классической МП ЛРП. Перед тем как перейти к доказательству теоремы 3, приведем пример ее использования.

Пусть $q = 3, R = \mathrm{GF}(q)$ — поле из трех элементов и α — корень неприводимого над R многочлена $x^2 + 2x + 2$ в поле $S = \mathrm{GF}(9)$. Пусть σ — автоморфизм Фробениуса S над R, действие которого на элементе $\mu \in S$ определено равенством $\sigma(\mu) = \mu^3$. Рассмотрим скрученную ЛРП v над S порядка 2 с характеристическим многочленом

$$\Psi(x) = x^2 - (2 + (2\alpha + 1)\sigma)\, x - (2 + (2\alpha + 1)\sigma) \in \check{S}[x]$$

и начальным вектором $(v(0), v(1)) = (0, 1)$. Таким образом, для всех $i \in \mathbb{N}_0$ в поле S имеет место равенство

$$v(i+2) = 2v(i+1) + (2\alpha+1)v(i+1)^3 + 2v(i) + (2\alpha+1)v(i)^3.$$

Непосредственной проверкой можно убедиться, что v — скрученная МП ЛРП и ее период равен $\mathbf{T} = |S|^2 - 1 = 80$. Первые 80 членов ЛРП v приведены в таблице ниже. Кроме того, имеют место равенства

$$\tau = \frac{\mathbf{T}}{q-1} = \frac{80}{3-1} = 40,\ v(i+40) = 2v(i).$$

Как будет показано далее (см. (2.3)), из последнего равенства следует, что $\gamma = 2 \in R$. Поэтому система равенств (1.16) имеет вид

$$|M_{0k}^{11}(v)| = |M_{0k}^{21}(v)|,\ |M_{0k}^{12}(v)| = |M_{0k}^{22}(v)|,\ k \in \overline{1, 39}. \tag{1.17}$$

Множества $M_{0k}^{11}(v), M_{0k}^{21}(v), M_{0k}^{12}(v), M_{0k}^{22}(v)$ перечислены в таблице ниже, и для них выполняется система равенств (1.17). Положим $K = \mathrm{GF}(7)$, пусть $f : S \to K$, отображение заданное по правилу

$$f(\mu) = \begin{cases} 0 & \mu \in S \setminus R, \\ 0 & \mu = 0, \\ 3 & \mu = 1, \\ 4 & \mu = 2. \end{cases}$$

Заметим, что последовательность $w(i) = f(\gamma^i)$ имеет вид $w = (3, 4, 3, 4, \ldots)$ и ее минимальный многочлен, равный $x + 1 \in K[x]$, взаимно прост с $x - 1$. Так как $f(w)$ есть ЛРП над полем, то $\mathrm{Ann} f(w)$ — главный идеал в кольце $K[x]$, т. е. $\mathrm{Ann}(f(w)) = K[x](x+1)$. Следовательно, по теореме 3

$$\mathrm{Ann} f(v) = K[x](x^{40} + 1). \tag{1.18}$$

Представленная ниже таблица содержит подтверждающие формулу (1.18) результаты вычислений с применением алгоритма Берлекэмпа – Месси (см., например, [33]).

2. Доказательства

Сначала докажем вспомогательный результат. Напомним, что θ — примитивный элемент поля K и $\vec{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ — базис пространства ${}_R S$.

Таблица

i	$v(i)$	i	$v(i)$	k	$M_{0k}^{11}(v)$	$M_{0k}^{21}(v)$	$M_{0k}^{12}(v)$	$M_{0k}^{22}(v)$
0	0	40	0	1	{34}	{48}	{8}	{74}
1	1	41	2	2	{32}	{75}	{35}	{72}
2	2α	42	α	3	{32}	{74}	{34}	{72}
3	$\alpha+1$	43	$2\alpha+2$	4	{77}	{9}	{49}	{37}
4	2α	44	α	5	{8}	{72}	{32}	{48}
5	2α	45	α	6	{26}	{75}	{35}	{66}
6	$\alpha+2$	46	$2\alpha+1$	7	{1}	{74}	{34}	{41}
7	α	47	2α	8	{26}	{41}	{1}	{66}
8	1	48	2	9	{26}	{72}	{32}	{66}
9	2	49	1	10	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
10	0	50	0	11	{77}	{66}	{26}	{37}
11	α	51	2α	12	{1}	{37}	{77}	{41}
12	$\alpha+2$	52	$2\alpha+1$	13	{13}	{75}	{35}	{53}
13	1	53	2	14	{35}	{74}	{34}	{75}
14	$\alpha+2$	54	$2\alpha+1$	15	{34}	{66}	{26}	{74}
15	$\alpha+2$	55	$2\alpha+1$	16	{77}	{72}	{32}	{37}
16	$\alpha+1$	56	$2\alpha+2$	17	{32}	{9}	{49}	{72}
17	$2\alpha+1$	57	$\alpha+2$	18	{8}	{75}	{35}	{48}
18	α	58	2α	19	{13}	{74}	{34}	{53}
19	2α	59	α	20	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
20	0	60	0	21	{13}	{72}	{32}	{53}
21	$2\alpha+1$	61	$\alpha+2$	22	{13}	{66}	{26}	{53}
22	$\alpha+1$	62	$2\alpha+2$	23	{26}	{9}	{49}	{66}
23	α	63	2α	24	{8}	{53}	{13}	{48}
24	$\alpha+1$	64	$2\alpha+2$	25	{1}	{9}	{49}	{41}
25	$\alpha+1$	65	$2\alpha+2$	26	{8}	{9}	{49}	{48}
26	1	66	2	27	{8}	{66}	{26}	{48}
27	$2\alpha+2$	67	$\alpha+1$	28	{49}	{53}	{13}	{9}
28	$2\alpha+1$	68	$\alpha+2$	29	{77}	{48}	{8}	{37}
29	$\alpha+2$	69	$2\alpha+1$	30	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
30	0	70	0	31	{1}	{75}	{35}	{41}
31	$2\alpha+2$	71	$\alpha+1$	32	{49}	{74}	{34}	{9}
32	1	72	2	33	{1}	{48}	{8}	{41}
33	$2\alpha+1$	73	$\alpha+2$	34	{1}	{72}	{32}	{41}
34	1	74	2	35	{77}	{53}	{13}	{37}
35	1	75	2	36	{13}	{41}	{1}	{53}
36	α	76	2α	37	{77}	{75}	{35}	{37}
37	2	77	1	38	{77}	{74}	{34}	{37}
38	$2\alpha+2$	78	$\alpha+1$	39	{49}	{75}	{35}	{9}
39	$\alpha+1$	79	$2\alpha+2$					

Лемма 4. *Пусть* $(\zeta_0, \ldots, \zeta_{n-1})$ — *линейно независимая система элементов пространства* ${}_RK$ *и* $w \in S^{\langle 1\rangle}$ — *последовательность вида*

$$w(i) = \alpha_0 \operatorname{tr}_R^K(\zeta_0\theta^i) + \alpha_1 \operatorname{tr}_R^K(\zeta_1\theta^i) + \ldots + \alpha_{n-1} \operatorname{tr}_R^K(\zeta_{n-1}\theta^i),\ i \geqslant 0.$$

Тогда для всех $k \in \mathbb{N}_0$, $s \in S^*$ *имеют место равенства*

$$|M_k^s(w)| = q^{n(m-1)}, \left|M_k^0\big(w\big)\right| = q^{n(m-1)} - 1.$$

Доказательство. Докажем лемму 4. Отметим, что w как сумма реверсивных последовательностей есть реверсивная последовательность [30]. Следовательно, достаточно провести доказательство для случая $k = 0$.

Для произвольного $s \in S^*$ существует единственный набор $(a_0, \ldots, a_{n-1}) \in R^n$ со свойством

$$s = \alpha_0 a_0 + \ldots + \alpha_{n-1} a_{n-1}.$$

Тогда равенство $w(i) = s$ равносильно системе равенств

$$\begin{cases} \mathrm{tr}_R^K(\zeta_0 \theta^i) = a_0, \\ \mathrm{tr}_R^K(\zeta_1 \theta^i) = a_1, \\ \vdots \\ \mathrm{tr}_R^K(\zeta_{n-1} \theta^i) = a_{n-1}. \end{cases} \tag{2.1}$$

Отметим, что определение числа решений системы (2.1) является классической задачей (см., например, [31, 32]). В данной работе мы приводим ее решение, базирующееся на применении двойственных базисов, отличное от представленных в [31, 32].

Найдем число решений $\theta^i \in K^*$ данной системы. Дополним линейно независимую систему $(\zeta_0, \ldots, \zeta_{n-1})$ до базиса $(\zeta_0, \ldots, \zeta_{n-1}, \zeta_n, \ldots, \zeta_{mn-1})$ пространства ${}_RK$. Пусть $\vec{\mu} = (\mu_0, \ldots, \mu_{mn-1})$ — базис, двойственный к базису $(\zeta_0, \ldots, \zeta_{mn-1})$ [1], т. е.

$$\mathrm{tr}_R^K(\zeta_j \mu_l) = \begin{cases} e, & j = l, \\ 0, & j \neq l, \end{cases}$$

где e — единица поля R. Пусть $\theta^i = \sum\limits_{j=0}^{mn-1} \mu_j c_j$ — разложение θ^i в базисе $\vec{\mu}$. Тогда система (2.1) равносильна системе равенств $c_j = a_j$ для $j \in \overline{0, n-1}$. При этом система (2.1) не накладывает ограничений на коэффициенты $c_n, \ldots, c_{mn-1}$. Поскольку θ — примитивный элемент поля K и не все элементы набора $(a_0, \ldots, a_{n-1})$ равны нулю, то каждый из коэффициентов $c_n, \ldots, c_{mn-1}$ может принимать произвольное значение из R. Таким образом, система (2.1) имеет $q^{mn-n} = q^{n(m-1)}$ решений.

В случае когда $(a_0, \ldots, a_{n-1})$ — нулевой набор, вектор $(c_n, \ldots, c_{mn-1})$ может быть любым ненулевым вектором из R^{mn-n}. В данном случае система (2.1) имеет $q^{mn-n} - 1$ решений. Лемма 4 доказана. □

Следствие 5. *Для $s \in S^*$, $k \in \mathbb{N}_0$ имеют место равенства*

$$M_k^s(v) = q^{n(m-1)}, \;\; M_k^0(v) = q^{n(m-1)} - 1.$$

Справедливость следствия 5 следует из леммы 4 и того, что система (1.12) есть базис пространства ${}_RK$.

2.1. Доказательство теоремы 3

Далее на множестве $\{0, 1, \ldots, \infty\}$ будем рассматривать операции

$$a \pm b = \begin{cases} a \pm b \pmod{q^{mn} - 1}, & \text{если } a \neq \infty,\ b \neq \infty, \\ \infty & \text{в противном случае.} \end{cases}$$

Определим также функцию $e : \mathbb{N}_0 \to \{0, 1, \ldots, q-2, \infty\}$

$$e(i) = \begin{cases} \infty, & v(i) \in (S \setminus R) \cup \{0\}, \\ \log_\gamma v(i), & v(i) \in R^*, \end{cases} \tag{2.2}$$

т. е. если $v(i) \in R^*$, то $v(i) = \gamma^{e(i)}$. Также по определению будем полагать $\beta^\infty = 0, \gamma^\infty = 0, x^\infty u = 0$ для произвольной последовательности u. Напомним, что через e мы обозначаем единицу поля S. Данное обозначение не должно вызывать путаницы в связи с использованием того же обозначения для функции (2.2), так как смысл подразумеваемого объекта всегда будет ясен из контекста.

Лемма 6. *Пусть $G(x) = \sum\limits_{k \geqslant 0} g_k x^k \in S[x]$. Тогда для произвольных $i, j \geqslant 0$ имеют место равенства*

$$G(x^\tau) f(v)(i + \tau j) = G(x) x^{e(i)} f(w)(j) = x^{e(i)} G(x) f(w)(j).$$

Доказательство. Докажем лемму 6. С учетом (1.11) для всех $k \in \mathbb{N}_0$ имеют место равенства

$$v(i + \tau k) = \sum_{l=0}^{n-1} \alpha_l \operatorname{tr}_R^K(\zeta_l \theta^{i+\tau k}) = \theta^{\tau k} \sum_{l=0}^{n-1} \alpha_l \operatorname{tr}_R^K(\zeta_l \theta^i) = \theta^{\tau k} v(i) = \gamma^k v(i). \tag{2.3}$$

Во втором равенстве выше мы воспользовались тем, что для всех $k \in \mathbb{N}_0$ имеет место включение $\theta^{\tau k} \in R$. Далее, с учетом (2.3) и (1.15)

получаем

$$G(x^\tau)f(v)(i+\tau j) = \sum_{k\geqslant 0} g_k x^{\tau k} f(v)(i+\tau j) = \sum_{k\geqslant 0} g_k f(v)(i+\tau j+\tau k)$$
$$= \sum_{k\geqslant 0} g_k f(\gamma^{j+k} v(i)) = \sum_{k\geqslant 0} g_k f(\gamma^{j+k}\gamma^{e(i)}) = \sum_{k\geqslant 0} g_k x^k x^{e(i)} f(\gamma^j)$$
$$= \sum_{k\geqslant 0} g_k x^k x^{e(i)} f(w)(j) = G(x)x^{e(i)} f(w)(j) = x^{e(i)} G(x) f(w)(j).$$

Лемма 6 доказана. □

Следствие 7. *Если* $G(x)f(w) = 0$, *то* $G(x^\tau)f(v) = 0$.

Доказательство. Действительно, с учетом леммы 6 для произвольных $i, j \in \mathbb{N}_0$ имеем

$$0 = x^{e(i)} G(x) f(w)(j) = G(x^\tau) f(v)(i+\tau j).$$

Следовательно, $G(x^\tau)f(v) = 0$. □

Лемма 8. *Пусть* $H(x) = \sum\limits_{k=0}^{\tau-1} H_k(x^\tau)x^k$ *и* $H(x)f(v) = 0$. *Тогда*

$$H_0(x)f(w) = 0.$$

Доказательство. Докажем лемму 8. Имеем $0 = H(x)f(v)$. Следовательно, для всех $i, j \geqslant 0$ имеют место равенства

$$0 = H(x)f(v)(i+\tau j) = \sum_{k=0}^{\tau-1} H_k(x^\tau)x^k f(v)(i+\tau j)$$
$$= \sum_{k=0}^{\tau-1} H_k(x^\tau) f(v)(i+k+\tau j).$$

С учетом леммы 6 получаем

$$0 = \sum_{k=0}^{\tau-1} H_k(x^\tau) f(v)(i+k+\tau j) = \sum_{k=0}^{\tau-1} H_k(x) x^{e(i+k)} f(w)(j). \qquad (2.4)$$

Суммируя равенства (2.4) по всем $i \in M_0^e(v)$, находим, что

$$0 = \sum_{i\in M_0^e} \sum_{k=0}^{\tau-1} H_k(x) x^{e(i+k)} f(w)(j)$$
$$= \sum_{i\in M_0^e} H_0(x) x^{e(i)} f(w)(j) + \sum_{i\in M_0^e} \sum_{k=1}^{\tau-1} H_k(x) x^{e(i+k)} f(w)(j)$$
$$= \sum_{i\in M_0^e} H_0(x) f(w)(j) + \sum_{i\in M_0^e} \sum_{k=1}^{\tau-1} H_k(x) x^{e(i+k)} f(w)(j).$$

По следствию 5 имеет место равенство $|M_0^e(v)| = q^{n(m-1)}$. Тогда в силу разложения

$$M_0^e(v) = \bigcup_{l\in\{0,1,\dots,q^n-2,\infty\}} M_{0k}^{e\beta^l}(v),\ k \in \overline{1,\tau-1},$$

получаем

$$0 = q^{n(m-1)}H_0(x)f(w)(j) + \sum_{k=1}^{\tau-1} H_k(x) \sum_{l\in\{0,1,\dots,q^n-2,\infty\}} \sum_{i\in M_{0k}^{e\beta^l}} x^{e(i+k)}f(w)(j).$$

С учетом (2.2) и (1.15) преобразуем второе слагаемое правой части последнего равенства

$$\begin{aligned}
&\sum_{k=1}^{\tau-1} H_k(x) \sum_{l\in\{0,1,\dots,q^n-2,\infty\}} \sum_{i\in M_{0k}^{e\beta^l}} x^{e(i+k)}f(w)(j)\\
&= \sum_{k=1}^{\tau-1} H_k(x) \sum_{l\in\{0,1,\dots,q^n-2\}} \sum_{i\in M_{0k}^{e\beta^l}} x^{e(i+k)}f(w)(j)\\
&= \sum_{k=1}^{\tau-1} H_k(x) \sum_{l\in\{0,1,\dots,q-2\}} \sum_{i\in M_{0k}^{e\gamma^l}} x^{e(i+k)}f(w)(j)\\
&= \sum_{k=1}^{\tau-1} H_k(x) \sum_{l\in\{0,1,\dots,q-2\}} \sum_{i\in M_{0k}^{e\gamma^l}} x^{l}f(w)(j).
\end{aligned}$$

Таким образом, получаем

$$0 = q^{n(m-1)}H_0(x)f(w)(j) + \sum_{k=1}^{\tau-1} H_k(x) \left(\sum_{l=0}^{q-2} |M_{0k}^{e\gamma^l}|x^l\right) f(w)(j). \qquad (2.5)$$

Суммируя равенства (2.4) по всем $i \in M_0^\gamma(v)$, аналогично устанавливаем

$$0 = q^{n(m-1)}H_0(x)f(w)(j+1) + \sum_{k=1}^{\tau-1} H_k(x) \left(\sum_{l=0}^{q-2} |M_{0k}^{\gamma\gamma^l}|x^l\right) f(w)(j). \quad (2.6)$$

Вычитая из равенства (2.6) равенство (2.5), с учетом (1.16) находим

$$0 = q^{n(m-1)}H_0(x)(f(w)(j+1) - f(w)(j)).$$

Последнее равенство перепишем в виде

$$0 = q^{n(m-1)}H_0(x)(x - \mathbf{e})f(w)(j).$$

Поскольку элемент $q\mathbf{e}$ не является делителем нуля в кольце K, имеет место равенство

$$0 = H_0(x)(x - \mathbf{e})f(w)(j). \tag{2.7}$$

Пусть $F(x) \in \mathrm{Ann}(f(w))$ — многочлен, взаимно простой с $x - \mathbf{e}$. Тогда существуют такие многочлены $U(x), V(x) \in K[x]$, что

$$U(x)F(x) + V(x)(x - \mathbf{e}) = \mathbf{e}. \tag{2.8}$$

Умножив обе части равенства (2.7) на $V(x)$, с учетом коммутативности кольца $K[x]$ и равенства (2.8) получим

$$0 = V(x)H_0(x)(x - \mathbf{e})f(w)(j) = H_0(x)\left(\mathbf{e} - U(x)F(x)\right)f(w)(j) = H_0(x)f(w)(j).$$

Лемма 8 доказана. □

Лемма 9. *Пусть* $H(x) = \sum\limits_{k=0}^{\tau-1} H_k(x^\tau)x^k$ *и* $H(x)f(v) = 0$. *Тогда*

$$H_0(x)f(w) = H_1(x)f(w) = \ldots = H_{\tau-1}(x)f(w) = 0.$$

Доказательство. По лемме 8 имеет место равенство $H_0(x)f(w) = 0$. Тогда по следствию 7

$$H_0(x^\tau)f(v) = 0.$$

Следовательно,

$$\left(xH_1(x^\tau) + x^2H_2(x^\tau) + \ldots + x^{\tau-1}H_\tau(x^\tau)\right)f(v) = 0.$$

Так как последовательность $f(v)$ является реверсивной, то

$$\left(H_1(x^\tau) + xH_2(x^\tau) + \ldots + x^{\tau-2}H_{\tau-1}(x^\tau)\right)f(v) = 0.$$

Отсюда по лемме 8 и следствию 7 находим

$$H_1(x)f(w) = 0,\ H_1(x^\tau)f(v) = 0.$$

Аналогично показываем, что $H_k(x)f(w) = 0$ для $k \in \overline{2, \tau - 1}$. Лемма 9 доказана. □

Вернемся к доказательству теоремы 3. Пусть $H(x) \in \mathrm{Ann}f(v)$, тогда по лемме 9 имеет место включение $H(x) \in (G(x)|G(x) \in \mathrm{Ann}f(w))$. Обратное включение следует из следствия 7. Теорема 3 доказана.

Автор выражает признательность О. В. Камловскому за ряд ценных замечаний.

Список литературы

[1] Лидл Р., Нидеррайтер Г., *Конечные поля*, М.: Мир, 1988, 830 с.

[2] Гольтваница 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.

[3] 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.

[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] Niederreiter H., "The multiple-recursive matrix method for pseudorandom number generation", *Finite Fields Appl.*, **1**:1 (1995), 3–30.

[6] Tsaban B., Vishne U., "Efficient linear feedback shift registers with maximal period", *Finite Fields Appl.*, **8**:2 (2002), 256–267.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Hasan S., Panario D., Wang Q., "Word-oriented transformation shift registers and their linear complexity", *Lect. Notes Comput. Sci.*, **7280** (2012), 190–201.

[12] Chen E., Tseng D., "The splitting subspace conjecture", *Finite Fields Appl.*, **24** (2013), 15–28.

[13] Zeng G., Yang Y., Han W., Fan S., "Word oriented cascade jump σ-LFSR", Lect. Notes Comput. Sci., **5527**, 2009, 127–136.

[14] 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.

[15] Гольтваница М.А., "Скрученные σ-разделимые линейные рекуррентные последовательности максимального периода", *Математические вопросы криптографии*, **13**:1 (2022), 33–67.

[16] Гольтваница 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.

[17] 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.

[18] Zaitcev S.N., "Description of maximal skew linear recurrences in terms of multipliers", *Математические вопросы криптографии*, **5**:2 (2014), 57–70.

[19] Зайцев С.Н., "Треугольный класс скрученных многочленов максимального периода", *Проблемы передачи информации*, **52**:4 (2016), 84–93.

[20] Нечаев А.А., "Код Кердока в циклической форме", *Дискретная математика*, **1**:4 (1989), 123–139.

[21] Goltvanitsa M.A., "Digit sequences of skew linear recurrences of maximal period over Galois rings", *Математические вопросы криптографии*, **6**:2 (2015), 19–27.

[22] 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.

[23] Goltvanitsa M.A., "Equidistant filters based on skew ML-sequences over fields", *Математические вопросы криптографии*, **9**:2 (2018), 71–86.

[24] 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.

[25] 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.

[26] Hassan S., Panario D., Wang Q., "Nonlinear vectorial primitive recursive sequences", *Cryptogr. Commun.*, **10**:6 (2018), 1075–1090.

[27] 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.

[28] Гольтваница М.А., "Новые представления знаков скрученных ЛРП при помощи функции след, базирующиеся на некоммутативной теореме Гамильтона – Кэли", *Математические вопросы криптографии*, **12**:1 (2021), 7–22.

[29] Куракин В.Л., "Представления линейных рекуррентных последовательностей максимального периода над конечным полем", *Дискретная математика*, **7**:2 (1995), 34–39.

[30] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра*, **2**, М.: Гелиос АРВ, 2003, 414 с.

[31] Кузьмин А.С., Куракин В.Л., Нечаев А.А., "Псевдослучайные и полилинейные последовательности", *Труды по дискретной математике*, **1** (1997), 139–202.

[32] Камловский О.В., "Оценки числа появлений векторов на циклах линейных рекуррентных последовательностей над конечным полем", *Дискретная математика*, **20**:4 (2008), 102–112.

[33] Куракин В.Л., "Алгоритм Берлекэмпа – Месси над конечными кольцами модулями и бимодулями", *Дискретная математика*, **10**:4 (1998), 3–34.