Math-Net.Ru

Общероссийский математический портал

М. А. Goltvanitsa, А. А. Nechaev, S. N. Zaitsev, Скошенные ЛРП максимального периода над кольцами Гауа, *Матем. вопр. криптогр.*, 2013, том 4, выпуск 2, 59–72

DOI: <https://doi.org/10.4213/mvk83>

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: 54.198.67.100

26 апреля 2023 г., 12:37:09

УДК: 512.53+519.113.6

Skew LRS of maximal period over Galois rings*

M. A. Goltvanitsa¹, A. A. Nechaev², S. N. Zaitsev¹

¹Moscow State Technical University of Radio Engineering,
Electronics and Automatics, Moscow

²Academy of Cryptography of the Russian Federation, Moscow

Получено 18.IX.2012

Let p be a prime number, $R = \text{GR}(q^d, p^d)$ be a Galois ring with $q^d = p^{rd}$ elements and characteristic p^d . Denote by $S = \text{GR}(q^{nd}, p^d)$ a Galois extension of the ring R of dimension n and by $\check{S}$ the ring of all linear transformations of the module ${}_R S$. A sequence v over the ring S satisfying the recursion $\forall i \in \mathbb{N}_0: v(i+m) = \psi_{m-1}(v(i+m-1)) + \dots + \psi_0(v(i))$, $\psi_0, \dots, \psi_{m-1} \in \check{S}$, is called a *skew LRS over S with a characteristic polynomial* $\Psi(x) = x^m - \sum_{t=0}^{m-1} \psi_t x^t \in \check{S}[x]$. We investigate the problem of construction the polynomials Ψ generating LRS v with the maximal possible period $\tau = (q^{mn} - 1)p^{d-1}$.

Key words: Galois ring, Frobenius automorphism, skew linear recurrence of maximal period, skew MP-polynomial, rank of a sequence

Скошенные ЛРП максимального периода над кольцами Галуа

М. А. Гольтованица¹, А. А. Нечаев², С. Н. Зайцев¹

¹Московский государственный технический университет радиотехники,
электроники и автоматики, Москва

²Академия криптографии Российской Федерации, Москва

Аннотация. Пусть p — простое число, $R = \text{GR}(q^d, p^d)$ — кольцо Галуа с $q^d = p^{rd}$ элементами и характеристикой p^d . Обозначим через $S = \text{GR}(q^{nd}, p^d)$ расширение Галуа кольца R размерности n и через $\check{S}$ — кольцо всех линейных преобразований модуля ${}_R S$. Последовательность v над кольцом S , удовлетворяющая соотношению $\forall i \in \mathbb{N}_0: v(i+m) = \psi_{m-1}(v(i+m-1)) + \dots + \psi_0(v(i))$, $\psi_0, \dots, \psi_{m-1} \in \check{S}$, называется *скошенной ЛРП над S с характеристическим многочленом* $\Psi(x) = x^m - \sum_{t=0}^{m-1} \psi_t x^t \in \check{S}[x]$. Изучаются способы построения многочленов Ψ , порождающих ЛРП v с максимально возможным периодом $\tau = (q^{mn} - 1)p^{d-1}$.

Ключевые слова: кольцо Галуа, автоморфизм Фробениуса, скошенная линейная рекуррентная последовательность максимального периода, скошенный МП-многочлен, ранг последовательности

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 2, pp. 59–72 (Russian).

© 2013 M. A. Goltvanitsa, A. A. Nechaev, S. N. Zaitsev

---

* The research was supported by the Academy of Cryptography of the Russian Federation.

1. Introduction

In what follows, $R = \text{GR}(q^d, p^d)$ is a Galois ring, $S = \text{GR}(q^{nd}, p^d)$ is a Galois extension of dimension $n \geq 2$ of the ring R [1, 3, 5].

It is known that the group $\text{Aut}(S/R)$ of automorphisms of the ring S over R is a cyclic group of order n . Let σ be a generating element of $\text{Aut}(S/R)$ and $\check{S} = S^\sigma \langle \sigma \rangle$ be the skew group ring of the group $\langle \sigma \rangle$ over the ring S , i. e. the set of formal sums $\psi = \sum_{i=0}^{n-1} s_i \sigma^i$, $s_0, \dots, s_{n-1} \in S$, with standard addition and with a multiplication defined by means of the distributive property and the identity

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

Each element $\psi \in \check{S}$ defines an endomorphism of the module ${}_R S$ such that $\psi(s) = \sum_{i=0}^{n-1} s_i \sigma^i(s)$ for every $s \in S$. So, we have the isomorphisms $\check{S} \cong \text{End}({}_R S) \cong R_{n,n}$, where $R_{n,n}$ is the ring of $n \times n$ -matrices over R . Thus, a structure of a left $\check{S}$ -module on S is given.

The set $S^{(1)}$ of all sequences $v: \mathbb{N}_0 \rightarrow S$ over S is a left module over the ring of polynomials $\check{S}[x]$, where the product of a sequence $v \in S^{(1)}$ by a polynomial $A(x) = \sum_{i \geq 0} a_i x^i \in \check{S}[x]$ is defined by the equality

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

We say that a sequence $v \in S^{(1)}$ is a *skew linear recurrent sequence (LRS)* of order m over S if it is LRS of order m over the module ${}_S S$ [4], i. e.

$$\Psi(x)v = 0$$

($\Psi(x)v$ is a zero sequence) for some monic polynomial $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$ of degree m . Such polynomial is called *skew characteristic polynomial of LRS v* . In other words, $v \in S^{(1)}$ is a skew LRS of order m over S if for some fixed $\psi_0, \dots, \psi_{m-1} \in \check{S}$ the following condition is fulfilled

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

For a fixed monic polynomial $\Psi(x) \in \check{S}[x]$ we shall denote by $L_S(\Psi)$ the set of all skew LRS (1) over S . Let us fix some basis $\vec{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ of the free module ${}_R S$ and denote by $a^\downarrow = (a_0, \dots, a_{n-1})^T \in R^{(n)}$ the column of coordinates of element $a \in S$ in the basis $\vec{\alpha}$:

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

Then each linear transformation $\psi \in \check{S}$ of the module ${}_R S$ is defined by some matrix $A(\psi) \in R_{n,n}$ such that for any $a \in S$

$$\psi(a)^\perp = A(\psi)a^\perp.$$

This matrix is called the *matrix of linear transformation ψ in the basis $\vec{\alpha}$* .

REMARK 1. If $\beta \in S$, then a homothety $\psi = \widehat{\beta}$, which maps $a \in S$ to the $\psi(a) = \widehat{\beta}(a) = \beta a$ is an invertible transformation (i.e. $A(\widehat{\beta})$ is an invertible matrix) iff β belongs to a multiplicative group S^* of the ring S . Moreover, if we denote by $\overline{A}$ the image of a matrix $A \in R_{n,n}$ under the natural epimorphism $R \rightarrow \overline{R} = R/pR = \text{GF}(q)$, then we can state that for every $\beta \in S$ a condition $A(\widehat{\beta}) \neq \overline{0}$ is equivalent to a condition that rank of the matrix $\overline{A(\widehat{\beta})}$ satisfies the equality

$$\text{rank } \overline{A(\widehat{\beta})} = n.$$

Evidently, the sequence $v \in S^{(1)}$ is a skew LRS of order m with the characteristic polynomial $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j$ if and only if the columns of coordinates $v^\perp(i)$ of items $v(i)$ of this sequence in the basis $\vec{\alpha}$ satisfy the relation

$$\forall i \in \mathbb{N}_0: v^\perp(i+m) = A(\psi_{m-1})v^\perp(i+m-1) + \dots + A(\psi_0)v^\perp(i). \quad (2)$$

We call relation (2) a *recursion law of a skew LRS v in a matrix form and polynomial*

$$\mathcal{A}(x) = x^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0 \in R_{n,n}[x], \quad A_s = A(\psi_s) \quad (3)$$

— a *skew characteristic polynomial of LRS v in a matrix form*.

Let us denote by $T(v)$ the period of a sequence $v \in S^{(1)}$ and by $T(F)$ the period of a monic polynomial $F(x) \in S[x]$ (the period of a sequence $e, x, \dots, x^i, \dots$ in the residue ring $S[x]/F(x)S[x]$ [2, 3]).

Proposition 1 ([13]). *For any skew monic polynomial $\Psi(x) \in \check{S}[x]$ of degree m there exists a monic polynomial $F(x) \in R[x]$ of degree mn such that*

$$L_S(\Psi) \subset L_S(F). \quad (4)$$

Thus, a period of any skew LRS $v \in L_S(\Psi)$ satisfies the following relations:

$$T(v) | T(F), \quad T(F) \leq \tau = (q^{nm} - 1)p^{d-1}. \quad (5)$$

Under the condition of Proposition 1 in the case $T(v) = \tau$ we say that v is a skew LRS of *maximal period* (MP LRS) and $\Psi(x)$ is a *skew MP-polynomial*.

The problem of description of all MP LRS is not solved. Some classes of MP-polynomials in matrix form over fields was discovered mainly by brute force method, see [4, 7–10].

Let us note that it was conjectured in [8] that (in our terms) the cardinality of the set $\text{SMP}_S(m)$ of all skew MP-polynomials of degree m over the field $S = \text{GF}(q^n)$ is

$$|\text{SMP}_S(m)| = \frac{\varphi(q^{nm} - 1)}{mn} (q^n - q) \dots (q^n - q^{n-1}) q^{n(n-1)(m-1)}. \quad (6)$$

This conjecture was checked for many values m, n, q , and proved in special cases: for $m = 1$ and any n, q (in [11]), for $n = 2$ and any m, q (in [12]).

2. Main results

In this paper a general characterization of the set of all skew MP LRS over a Galois ring is proposed, a simple method of construction of large classes of skew MP-polynomials is given and ranks of skew MP LRS as linear recurrent sequences over modules ${}_S S$ and ${}_R S$ are calculated.

This section contains statements of all our results, including results of recently published work [13]. The next section contains proofs of new results.

Let us fix a basis $\vec{\alpha}$ of the module ${}_R S$. Then any sequence $v \in S^{(1)}$ defines the collection of sequences $v_0, \dots, v_{n-1} \in R^{(1)}$ such that

$$v = v_0 \alpha_0 + v_1 \alpha_1 + \dots + v_{n-1} \alpha_{n-1}. \quad (7)$$

We call $v_0, \dots, v_{n-1}$ the *coordinate sequences* of the sequence v (in the basis $\vec{\alpha}$). In what follows, we use the notation $u[\overline{i, i+k}] = (u(i), \dots, u(i+k))$ for all $u \in S^{(1)}$, $i, k \in \mathbb{N}_0$.

Theorem 1 ([13]). *A sequence $v \in S^{(1)}$ is a skew MP LRS of order m over the ring S if and only if*

$$\forall i \in \mathbb{N}_0: v[\overline{i, i+m-1}] \notin (pS)^m, \quad (8)$$

and there exists an MP-polynomial $F(x) \in R[x]$ of degree mn such that

$$v \in L_S(F). \quad (9)$$

Each skew MP LRS v is a reversible (pure periodic) one and under condition (9) the system of its coordinate sequences $v_0, \dots, v_{n-1}$ from decomposition (7) is a linearly independent system of MP LRS in $L_R(F(x))$.

The following result gives the first concrete method of construction of a skew MP-polynomials class from one skew MP-polynomial.

Theorem 2 ([13]). *Let v be a skew MP LRS of order m over S with characteristic polynomial $\Psi(x) = x^m - \sum_{i=0}^{m-1} \psi_i x^i \in \check{S}[x]$, ψ be a transformation from $\check{S}$, and $w = \psi(v)$ be a sequence of elements $w(i) = \psi(v(i))$, $i \in \mathbb{N}_0$. Then*

(a) *if $\psi \in \check{S}^*$, then w is a skew MP LRS with characteristic polynomial $\Psi'(x) = x^m - \sum_{i=0}^{m-1} (\psi \cdot \psi_i \cdot \psi^{-1}) x^i$;*

(b) *if w is an MP LRS over S , then $\psi \in \check{S}^*$.*

2.1. Linearized skew MP-polynomials

Under the condition of Theorem 2(a), if v is a classic MP LRS of order m over the ring S of maximal period τ , i. e. if $\Psi(x) \in S[x]$, we say that a skew MP LRS $w = \psi(v)$ and the polynomial $\Psi' \in \check{S}[x]$ are *linearized*.

Let us denote by $\text{LMP}_S(m)$ and $\text{MP}_S(m)$ the set of all linearized MP-polynomials $\Psi(x) \in \check{S}[x]$ of degree m and the set of all MP-polynomials $G(x) \in S[x]$ of degree m , correspondingly. Denote by φ the Euler totient function.

Theorem 3 ([13]). *The set $\text{LMP}_S(m)$ has a cardinality*

$$|\text{LMP}_S(m)| = |\text{MP}_S(m)| \frac{|R_{n,n}^*|}{n|S^*|} = \frac{\varphi(q^{nm} - 1)(q^n - q) \dots (q^n - q^{n-1}) q^{(d-1)n^2}}{nmq^{n(d-1)}} \Delta,$$

where

$$\Delta = \begin{cases} 1, & \text{if } d = 1; \\ (q^{nm} - 1)q^{nm(d-2)}, & \text{if } d > 1, p > 2 \text{ or } p = d = 2; \\ (q^{nm} - 2)q^{nm(d-2)}, & \text{if } p = 2 < d. \end{cases} \quad (10)$$

Corollary 1. *If $d = 1$, i.e. $R = \text{GF}(q)$, $S = \text{GF}(q^n)$, then*

$$|\text{LMP}_S(m)| = \frac{\varphi(q^{nm} - 1)}{nm} (q^n - q) \dots (q^n - q^{n-1}).$$

Comparison of the last formula with conjecture (6) shows that the class of linearized skew MP-polynomials is essentially smaller than the class of all skew MP-polynomials.

2.2. Some constructions of non-linearized skew MP-polynomials

The following approach to the construction of skew MP-polynomials is developed.

Theorem 4. Let $K = \text{GR}(q^{nmd}, p^d)$ be a Galois extension of the ring S and θ be some element of maximal order $\tau = (q^{mn} - 1)p^{d-1}$ from K^* . Let $a_0, \dots, a_{n-1} \in K$ be such elements that the system

$$\begin{aligned} \vec{\theta} = \vec{\theta}(a_0, \dots, a_{n-1}) = \\ = (a_0, \dots, a_{n-1}, a_0\theta, \dots, a_{n-1}\theta, \dots, a_0\theta^{m-1}, \dots, a_{n-1}\theta^{m-1}) \end{aligned} \quad (11)$$

be a basis of the module ${}_R K$, and the matrix $B \in R_{mn, mn}$ satisfy the relation

$$B\theta^\downarrow = \theta\theta^\downarrow, \quad (12)$$

where $\theta^\downarrow = \vec{\theta}^T$. Let matrices $A_0, \dots, A_{m-1} \in R_{n, n}$ be defined by the last n rows of the matrix B from the equality

$$(A_0, \dots, A_{m-1}) = \begin{pmatrix} \vec{B}_{(m-1)n+1} \\ \vdots \\ \vec{B}_{mn} \end{pmatrix}. \quad (13)$$

Then

$$\mathcal{A}(x) = x^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0$$

is a skew MP-polynomial in a matrix form.

The construction of skew MP-polynomials in this subsection is based on the construction of some basis (11) of the free module ${}_R K$ with further application of theorem 4.

Theorem 5. Let $m > 1$ and

$$F(x) = x^{mn} - f_{mn-1}x^{mn-1} - \dots - f_1x - f_0 \in R[x] \quad (14)$$

be an MP-polynomial. Then a polynomial $\mathcal{A}(x) \in R_{n, n}[x]$ of the form

$$\mathcal{A}(x) = x^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0, \quad (15)$$

where

$$A_0 = \begin{pmatrix} 0 & e & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e \\ f_0 & f_m & \dots & f_{(n-1)m} \end{pmatrix}, \quad A_t = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \\ f_t & f_{m+t} & \dots & f_{(n-1)m+t} \end{pmatrix}, \quad (16)$$

$t \in \{1, \dots, m-1\}$, is a non-linearized skew MP-polynomial.

Theorem 6. Let $m > 1$, $n > 2$ and $F(x)$ be an MP-polynomial (14) such that there exists $t = jm$, $j \in \{1, \dots, n-1\}$, with the property¹

$$\hat{f}_t \in R^*. \quad (17)$$

Let a map $h: \{0, \dots, mn-1\} \rightarrow \{0, \dots, mn\}$ be defined by the rule

$$h(kn+l) = \begin{cases} lm+k, & \text{if } l < j, \\ lm+k+1, & \text{if } l \geq j, \end{cases} \quad (18)$$

for all $k \in \{0, \dots, m-1\}$, $l \in \{0, \dots, n-1\}$, and let matrices $A_0, \dots, A_{m-1} \in R_{n,n}$ be defined in the following way:

$$A_0 = \begin{matrix} & j & \\ \begin{matrix} 0 & e & 0 & 0 & \dots & \dots & 0 & 0 & 0 \\ 0 & 0 & e & 0 & \dots & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \ddots & \dots & \dots & \dots & \dots & \dots \\ a_{h(0)} & a_{h(1)} & \dots & \dots & a_{h(j-1)} & a_{h(j)} & \dots & \dots & a_{h(n-1)} \\ 0 & \dots & \dots & \dots & 0 & e & 0 & \dots & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 & e \\ n & c_{h(0)} & c_{h(1)} & \dots & \dots & \dots & \dots & \dots & c_{h(n-1)} \end{matrix} & \end{matrix}, \quad (19)$$

$$A_s = \begin{matrix} & j & \\ \begin{matrix} 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \\ a_{h(ns)} & a_{h(ns+1)} & \dots & \dots & a_{h(ns+n-1)} \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \\ n & c_{h(ns)} & c_{h(ns+1)} & \dots & \dots & c_{h(ns+n-1)} \end{matrix} & \end{matrix}, \quad 1 \leq s < m, \quad (20)$$

where

$$a_{h(k)} = \begin{cases} \hat{f}_{jm}^{-1}, & \text{if } h(k) = mn, \\ -\hat{f}_{jm}^{-1} \hat{f}_{h(k)}, & \text{if } h(k) \neq mn, \end{cases} \quad (21)$$

¹ The analysis of the table of irreducible polynomials from [6] shows that such polynomials exist for any values m, n, q , except for $m = n = q = 2$.

$$c_{h(k)} = \begin{cases} -f_{jm-1}f_{jm}^{-1}f_0, & \text{if } h(k) = 0, \\ f_{jm-1}f_{jm}^{-1} + f_{mn-1}, & \text{if } h(k) = mn, \\ f_{h(k)-1} - f_{h(k)}f_{jm-1}f_{jm}^{-1}, & \text{if } h(k) \notin \{0, mn\}. \end{cases} \quad (22)$$

Then a polynomial

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

is a skew non-linearized MP-polynomial in a matrix form.

2.3. Ranks of a skew MP LRS

Let us denote by $\text{rk}_S v$, $\text{rk}_R v$, the rank (the degree of minimal polynomial) of a sequence $v \in S^{(1)}$ as LRS over modules ${}_S S$ and ${}_R S$, respectively (see [3]).

Theorem 1 implies that for any skew MP LRS v over the ring S the equality $\text{rk}_R v = mn$ is true. If v is a classic MP LRS over the ring S , then by definition $\text{rk}_S v = m$. If v is a skew MP LRS over S we have the following inequalities:

$$m \leq \text{rk}_S v \leq mn. \quad (23)$$

Here left inequality is strict except the “trivial” case (when v is a classic MP LRS over ${}_S S$) and right inequality in some cases becomes an equality.

To formulate the general result let us denote by $\overline{S}$ the quotient field

$$\overline{S} = S/pS = \text{GF}(q^n)$$

and by $\bar{a}$ the image of an element $a \in S$ under the natural epimorphism $S \rightarrow \overline{S}$. Note that every linear transformation $\psi \in \check{S}$ of module ${}_R S$ induces a linear transformation $\bar{\psi} \in \check{\overline{S}}$ of space ${}_R \overline{S}$ by the rule

$$\forall a \in S: \bar{\psi}(\bar{a}) = \overline{\psi(a)}.$$

The correspondence $\psi \rightarrow \bar{\psi}$ gives an epimorphism of rings $\check{S} \rightarrow \check{\overline{S}}$ with the kernel $p\check{S}$.

Theorem 7 ([13]). *Let v be a skew MP LRS of order m over S with the characteristic polynomial $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$ such that*

$$\overline{\Psi}(x) = x^m - \sum_{j=0}^{m-1} \bar{\psi}_j x^j \notin \overline{S}[x]. \quad (24)$$

Then $\text{rk}_S v = km$ for some $k \in \{2, \dots, n\}$.

The rank of linearized MP LRS may be estimated more exactly. Let us define the *Hamming weight* of any element

$$\psi = \sum_{l=0}^{n-1} s_l \sigma^l \in \check{S} \quad (25)$$

by the equality $W(\psi) = |\{l \in \{0, \dots, n-1\} : s_l \neq 0\}|$. For any polynomial $G(x) = \sum_{j \geq 0} g_j x^j \in S[x]$ we put $\sigma(G(x)) = \sum_{j \geq 0} \sigma(g_j) x^j$.

Theorem 8 ([13]). *Let $u \in L_S(G(x))$, where $G(x)$ is an MP-polynomial of degree m over the ring S . Then for any $\psi \in \check{S}^*$ the sequence $v = \psi(u)$ is a skew MP LRS over S , $\text{rk}_S v = mW(\psi)$ and the polynomial*

$$M(x) = \prod_{l \in \overline{0, n-1} : s_l \neq 0} \sigma^l(G(x)) \quad (26)$$

is the minimal polynomial of LRS v over S .

If $W(\psi) = n$, then $\text{rk}_S v = \text{rk}_R v = mn$ and $M(x)$ is a polynomial of maximal period of degree mn over the ring R ; if moreover the transformation (25) satisfies the condition

$$s_0, \dots, s_{n-1} \in S^*, \quad (27)$$

then $M(x) \in R[x]$ is a unique minimal polynomial of the LRS v over S .

3. Proofs

3.1. Proof of theorem 4

It is known from [3] that θ is a root of some MP-polynomial

$$F(x) = x^{mn} - f_{mn-1} x^{mn-1} - f_1 x - f_0 \in R[x]. \quad (28)$$

Let $v_k \in L_R(F)$ be a sequence of the form

$$v_k(i) = \text{Tr}_R^K(a_k \theta^i), \quad i \geq 0, \quad k = 0, 1, \dots, n-1,$$

where Tr_R^K is a trace-function from the ring K onto the ring R [3, 5]. Let $v \in L_S(F)$ be a sequence with coordinate sequences $v_0, \dots, v_{n-1}$ in the basis $\vec{\alpha}$, i.e (7) holds:

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

Since $\vec{\theta}$ is a basis of the free module ${}_R K$, we obtain $a_j \notin pK$, $j = 0, 1, \dots, n-1$, and $T(v) = \text{ord } \theta = \tau$. Now in order to prove Theorem 4 it is enough to prove the validity of the condition

$$\forall i \in \mathbb{N}_0 \quad v^\downarrow(i+m) = A_0 v^\downarrow(i) + \dots + A_{m-1} v^\downarrow(i+m-1). \quad (29)$$

Condition (12) imply

$$B \cdot \text{Tr}_R^K(\theta^i \theta^\downarrow) = \text{Tr}_R^K(\theta^{i+1} \theta^\downarrow), \quad i \geq 0,$$

(here the function Tr operates on the vectors coordinate-wise). Hence,

$$\begin{aligned} B(v_0(i), \dots, v_{n-1}(i), \dots, v_0(m-1+i), \dots, v_{n-1}(m-1+i))^T = \\ = (v_0(i+1), \dots, v_{n-1}(i+1), \dots, v_0(m+i), \dots, v_{n-1}(m+i))^T. \end{aligned} \quad (30)$$

Let us denote

$$\begin{aligned} v^\downarrow(i) &= (\vec{v}(i), \vec{v}(i+1), \dots, \vec{v}(i+m-1))^T = \\ &= (v_0(i), \dots, v_{n-1}(i), v_0(i+1), \dots, v_{n-1}(i+1), \dots, v_{n-1}(i+m-1))^T. \end{aligned} \quad (31)$$

Then condition (30) has a form

$$Bv^\downarrow(i) = v^\downarrow(i+1). \quad (32)$$

Now in view of (13) the consecutive application of conditions (32), (31) imply the equality

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

which is equivalent to (29).

3.2. Proof of theorem 5

Let θ be a root of the polynomial $F(x)$ in the extension $K = \text{GR}(q^{nmd}, p^d)$ of the ring S [2, 5]. Then

$$(e, \theta, \dots, \theta^{mn-1}) \quad (33)$$

is a basis of the free module ${}_R K$. In notations of theorem 4 we put

$$(a_0, \dots, a_{n-1}) = (e, \theta^m, \dots, \theta^{m(n-1)}).$$

Then

$$\begin{aligned}\vec{\theta} &= \vec{\theta}(e, \theta^m, \dots, \theta^{m(n-1)}) = \\ &= (e, \theta^m, \dots, \theta^{m(n-1)}, \theta, \theta^{m+1}, \dots, \theta^{m(n-1)+1}, \dots, \theta^{m-1}, \dots, \theta^{mn-1})\end{aligned}\quad (34)$$

is a basis of the module ${}_R K$ (permutation of the basis (33)) and the matrix B in (12) looks like

$$B = \begin{pmatrix} & \mathbb{O} & & E & & \dots & & \mathbb{O} \\ & \vdots & & \vdots & & \ddots & & \vdots \\ & \mathbb{O} & & \mathbb{O} & & \dots & & E \\ 0 & e & \dots & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ f_0 & f_m & \dots & f_{(n-1)m} & f_1 & \dots & f_{(n-1)m+1} & \dots & f_{m-1} & \dots & f_{mn-1} \end{pmatrix}, \quad (35)$$

where $E, \mathbb{O} \in R_{n,n}$ are identity and zero matrices, correspondingly. Therefore, by theorem 4, the polynomial $\mathcal{A}(x)$ of the form (15) is a skew MP-polynomial.

Let us show that $\mathcal{A}(x)$ is a non-linearized skew MP-polynomial.

Lemma 1. *If a polynomial (3) is some linearized skew polynomial in a matrix form, then*

$$\forall k \in \{0, \dots, m-1\}: \overline{A}_k \neq \overline{0}; \Rightarrow \text{rank } \overline{A}_k = n.$$

□ Really, theorem 2 (a) and remark 1 imply that

$$A_k = U^{-1} A(\widehat{\beta}_k) U, \quad \beta_k \in S, \quad k = 0, 1, \dots, m-1,$$

for some $U \in R_{n,n}^*$. Now the necessary implication follows from remark 1. □

To prove that $\mathcal{A}(x)$ in the case considered is a non-linearized skew MP-polynomial we note that in view of (16)

$$\text{rank } \overline{A}_t \leq 1 < n, \quad t \in \{1, \dots, m-1\}. \quad (36)$$

So, if we assume that $\mathcal{A}(x)$ is a linearized skew MP-polynomial, then according to lemma 1

$$\overline{A}_1 = \dots = \overline{A}_{m-1} = \overline{0}.$$

In view of (16) it means that the image $\overline{F}(x) \in \overline{R}[x]$ of a polynomial $F(x)$ under the natural epimorphism $R \rightarrow \overline{R}$ has a form $\overline{F}(x) = \overline{G}(x^m)$. But since $m > 1$, we obtain that $\overline{F}(x)$ cannot be an MP-polynomial over $\overline{R}$ [6]. Therefore $F(x)$ is not an MP-polynomial over R [2, 3, 5]. Contradiction.

3.3. Proof of theorem 6

Let θ be a root of the polynomial $F(x)$ in the extension $K = \text{GR}(q^{nmd}, p^d)$ of the ring S [2, 5]. Let us show that a system of elements

$$\vec{\theta} = (\theta^{h(0)}, \theta^{h(1)}, \dots, \theta^{h(mn-1)})$$

is a basis of the module ${}_R K$. Really, it consists of the elements

$$e, \theta, \dots, \theta^{im-1}, \theta^{im+1}, \dots, \theta^{nm}$$

and is equivalent to the basis $(e, \theta, \dots, \theta^{nm-1})$ because (17), (21) allows to write down the equations

$$\theta^{jm} = f_{jm}^{-1}(\theta^{mn} - \sum_{k=0, k \neq jm}^{mn-1} f_k \theta^k) = \sum_{k=0}^{mn-1} a_{h(k)} \theta^{h(k)}. \quad (37)$$

It is easy to see that (18) imply

$$\forall k \in \{0, \dots, m-1\}, l \in \{0, \dots, n-1\}: h(l) + k = h(kn + l).$$

Therefore, if $a_0 = \theta^{h(0)}, \dots, a_{n-1} = \theta^{h(n-1)}$, then $a_l \theta^k = \theta^{h(kn+l)}$ and

$$\vec{\theta} = \vec{\theta}(a_0, \dots, a_{n-1}) = (\theta^{h(0)}, \theta^{h(1)}, \dots, \theta^{h(mn-1)}) \quad (38)$$

is a basis of the module ${}_R S$ from the condition of theorem 4. Let us use theorem 4 and find $\vec{B}_{(m-1)n+1}, \dots, \vec{B}_{mn}$ from (13).

Note that rows of a matrix B are numbered by $1, \dots, mn$.

So, a row $\vec{B}_{(m-1)n+s}$ is calculated from a relation

$$\theta \theta^{h((m-1)n+s-1)} = \vec{B}_{(m-1)n+s} \theta^\downarrow, \quad s \in \{1, \dots, n\}. \quad (39)$$

Lemma 2. If $s \in \{1, \dots, n\}$, $s \neq j$, $s \neq n$, then

$$\vec{B}_{(m-1)n+s} = (\underbrace{0 \dots 0}_s e 0 \dots 0). \quad (40)$$

□ According to (18),

$$h((m-1)n + s - 1) = \begin{cases} sm - 1, & \text{if } s - 1 < j, \\ sm, & \text{if } s - 1 \geq j; \end{cases} \quad (41)$$

and since $s < n$, we obtain

$$h(s) = \begin{cases} sm, & \text{if } s < j, \\ sm + 1, & \text{if } s \geq j. \end{cases} \quad (42)$$

Let us note now that the condition $s \neq j$ implies

$$s - 1 < j \iff s < j, \quad s - 1 \geq j \iff s \geq j$$

and, therefore, (41), (42) imply $h(s) = h((m-1)n + s - 1) + 1$. Hence, $\theta\theta^{h((m-1)n+s-1)} = \theta^{h(s)}$ and (40) follows from (39). □

In the cases $s = j$ and $s = n$ we get using (13), (38) and (39)

$$\theta\theta^{h((m-1)n+j-1)} = \theta^{jm} = \vec{B}_{(m-1)n+j}\theta^\downarrow = \sum_{l=0}^{mn-1} b_{(m-1)n+j,l}\theta^{h(l)}. \quad (43)$$

Now the equality $b_{(m-1)n+j,l} = a_{h(l)}$, $l \in \{0, \dots, mn-1\}$, follows from (37) and (43), so, $\vec{B}_{(m-1)n+j}$ is determined. The description of $\vec{B}_{mn}$ follows similarly from the chain of equalities

$$\theta\theta^{h((m-1)n+n-1)} = \theta^{mn+1} = \vec{f}_{jm-1}\theta^{jm} + \sum_{l=1, l \neq jm}^{mn} \vec{f}_{l-1}\theta^l = \sum_{l=0}^{mn-1} b_{mn,l}\theta^{h(l)}.$$

So, according to (21) we have $b_{mn,l} = c_{h(l)}$, $l \in \{0, \dots, mn-1\}$, where $c_{h(l)}$ are defined by (22). The validity of (13) for the matrices $A_0, \dots, A_{m-1}$ from (19), (20) is proved. So, by theorem 4 the polynomial $\mathcal{A}(x)$ is a skew MP-polynomial.

Let us prove that $\mathcal{A}(x)$ is a non-linearized skew MP-polynomial. It follows from (21) that $\vec{A}_{m-1} \neq \vec{0}$ since

$$\overrightarrow{(\vec{A}_{m-1})_j} = (a_{h(n(m-1))}, a_{h(n(m-1)+1)}, \dots, a_{h(mn-1)})$$

and $a_{h(mn-1)} = a_{mn} = \vec{f}_{jm}^{-1} \in R^*$. So,

$$0 < \text{rank} \vec{A}_{m-1} \leq 2 < n,$$

and by lemma 1 $\mathcal{A}(x)$ is a skew non-linearized MP-polynomial. Theorem 6 is proved.

Acknowledgement

Authors are sincerely grateful to the reviewer for the valuable remarks allowed to improve a style of the manuscript.

References

1. *Nechaev A. A.* Finite principal ideal rings // *Math. Sb.* — 1973. — V. 91. No. 3. — P. 350–366 (in Russian); English transl. in: *Math. USSR Sb.* — 1973. — V. 20. — P. 364–382.
2. *Nechaev A. A.* Cycle types of linear substitutions over finite commutative rings // *Math. Sb.* — 1994. — V. 78. No. 2. — P. 283–311 (transl. from *Mat. Sb.* — 1993. — V. 184. No. 3. — P. 21–56).
3. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules // *J. Math. Sci.* — 1995. — V. 76. No. 6. — P. 2793–2915.
4. *Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyshev V. N.* Linear and polylinear recurring sequences over Abelian groups and modules // *J. Math. Sci.* — 2000. — V. 102. No. 6. — P. 4598–4626.
5. *Nechaev A. A.* Finite Rings with Applications // In: *Handbook of Algebra* (Edited by Hazewinkel M., Elsevier B. V.). — 2008. — V. 5. — P. 213–320.
6. *Lidl R., Niederreiter H.* Finite Fields. — *Encyclopedia of Mathematics and its Applications.* — Cambridge University Press, 1983. — V. 20.
7. *Tsaban B., Vishne U.* Efficient linear feedback shift registers with maximal period // *Finite Fields and Their Appl.* — 2002. — V. 8. No. 2. — P. 256–267.
8. *Zeng G., Han W., He K. C.* High efficiency feedback shift register: σ -LFSR // *Cryptology ePrint Archive, Report 2007/114* (2007).
9. *Zeng G., He K. C., Han W.* A trinomial type of σ -LFSR oriented toward software implementation // *Science in China Series F-Inf. Sci.* — 2007. — V. 50. No. 3. — P. 359–372.
10. *Zeng G., He K. C., Han W.* Word oriented cascade jump σ -LFSR (Edited by Bras-Amoros, M., Hoholdt, T.) // *Lect. Notes Comput. Sci.* — 2009. — V. 5527. — P. 127–136.
11. *Ghorpade S. R., Hasan S. U., Kumari M.* Primitive polynomials, Singer cycles, and word-oriented linear feedback shift registers // *Des., Codes Cryptogr.* — 2011. — V. 58. No. 2. — P. 123–134.
12. *Ghorpade S. R., Ram S.* Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields // *Finite Fields Appl.* — 2011. — V. 17. No. 5. — P. 461–472.
13. *Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N.* Skew linear recurring sequences of maximal period over Galois rings // *Fund. Prikl. Matem.* — 2011/2012. — V. 17. No. 3. — P. 5–23. CNIT MSU (in Russian); *J. Math. Sci.* — 2012. — V. 187. No. 2. — P. 115–128.