

Description of maximal skew linear recurrences in terms of multipliers

S. N. Zaitsev

LLC "Certification Research Center", Moscow

Received 25.09.2013

Let $P = \text{GF}(q)$ be a field, $F = \text{GF}(q^n)$ be an extension of P . We construct a wide class of skew MP-polynomials over F by the description of multipliers of skew MP LRS. For P -skew MP LRS v over F we call linear transformation ψ (*generalized multiplier*) if there exists a number $l \geq 0$ such that $\psi(v(i)) = v(i+l)$, $i \geq 0$. Denote by $\mathfrak{M}(v)^*$ the set of all multipliers of a skew MP LRS v , and $\mathfrak{M}(v) = \mathfrak{M}(v)^* \cup \{0\}$. It is proved that $\mathfrak{M}(v)$ is a field and $\mathfrak{M}(v) \cong F$ if and only if v is linearized. Sufficient conditions for $\mathfrak{M}(v) \cong P$ are given. It is proved that for any P -skew MP LRS v there exists a transformation ψ such that the sequence $\psi(v)$ is $\mathfrak{M}(v)$ -skew MP LRS of the same order, and for any field $K < F$ there exists MP LRS v such that $\mathfrak{M}(v) \cong K$.

Keywords: skew linear recurrence, skew polynomial of maximal period, generalized multiplier, maximal non-reducible sequence.

Описание скрученных линейных рекуррент максимального периода в терминах мультипликаторов

С. Н. Зайцев

ООО "Центр сертификационных исследований", Москва

Аннотация. Пусть $P = \text{GF}(q)$ — поле, $F = \text{GF}(q^n)$ — его расширение. Предложен метод построения широкого класса скрученных МП-многочленов над F , который основан на описании мультипликаторов скрученных МП ЛРП. Для P -скрученной МП ЛРП над F преобразование ψ называется (*обобщенным мультипликатором*), если найдется число $l \geq 0$, для которого $\psi(v(i)) = v(i+l)$, $i \geq 0$. Обозначим через $\mathfrak{M}(v)^*$ множество всех мультипликаторов скрученной МП ЛРП v , пусть $\mathfrak{M}(v) = \mathfrak{M}(v)^* \cup \{0\}$. Доказано, что $\mathfrak{M}(v)$ — поле, и $\mathfrak{M}(v) \cong F$ тогда и только тогда, когда v линеаризуема. Предоставлены некоторые достаточные условия того, что $\mathfrak{M}(v) \cong P$. Доказано, что для любой P -скрученной МП ЛРП v найдется такое преобразование ψ такое, что $\psi(v)$ есть $\mathfrak{M}(v)$ -скрученная МП ЛРП того же порядка, и для любого поля $K < F$ найдется МП ЛРП такая v , что $\mathfrak{M}(v) \cong K$.

Ключевые слова: скрученные линейные рекурренты, скрученный многочлен максимального периода, обобщенный мультипликатор, максимально неприводимая последовательность.

1 Introduction

Let $P = \text{GF}(q)$ be a field of q elements, $F = \text{GF}(q^n)$ be an extension of P and $F^{(1)}$ be the set of all sequences over F . Denote by \mathcal{L} the ring $\mathcal{L}({}_P F)$ of all linear transformations of the space ${}_P F$. Let us define the product of a sequence $v \in F^{(1)}$ by a polynomial $\Psi(x) = \sum_{j \geq 0} \psi_j x^j \in \mathcal{L}[x]$ by the equality

$$\Psi(x)v = w \in F^{(1)} : w(i) = \sum_{j \geq 0} \psi_j (v(j+i)) \text{ for all } i \geq 0.$$

A sequence $v \in F^{(1)}$ is called (P -)skew LRS over the field F of order m , if there exists a monic polynomial $\Psi(x) \in \mathcal{L}[x]$ of degree m such that

$$\Psi(x)v = 0, \tag{1.1}$$

i.e. if v is LRS of order m over the module ${}_L F$.

In this case the polynomial $\Psi(x)$ is called *characteristic polynomial of LRS v* . In a particular case, when $\Psi(x) \in F[x]$ the sequence v is called *classic LRS*. (Here and further we'll identify F and the set of homotheties generating by the elements of F in \mathcal{L} .)

It is evident, that period $T(v)$ of the skew LRS v of order m over the field F is not greater than $\tau = |F|^m - 1 = q^{mn} - 1$. If $T(v) = \tau$, then the sequence v is reversible and is called *a skew LRS of maximal period (MP LRS)* [3].

For any sequence $v \in F^{(1)}$ and any transformation $\psi \in \mathcal{L}$ we define the sequence $\psi(v)$ by equalities

$$\psi(v)(i) = \psi(v(i)), \quad i \geq 0. \tag{1.2}$$

We say that sequences $u, v \in F^{(1)}$ are (P -)linearly equivalent, if there exists an invertible transformation $\psi \in \mathcal{L}^*$ such that $v = \psi(u)$. If a skew LRS v is linearly equivalent to some classic MP LRS over the field F , we say that the sequence v is a *linearized* one.

Note that until recently skew MP LRS were found only for some fixed parameters (q, n, m) by brute force method over fields [16]-[22].

In [3] general characterization of the class of all MP LRS over Galois rings and of the class of linearized MP LRS given. Coordinate sequences of MP LRS were also was investigated.

Here we'll construct a wider class of MP LRS over Galois field, which is based on the description of multipliers of skew MP LRS.

2 Main results

Let us fix some basis $\vec{\alpha} = (\alpha_0, \dots, \alpha_{n-1})$ of the space ${}_P F$ and denote by $a^\downarrow = (a_0, \dots, a_{n-1})^T \in P^n$ the column of coordinates of element $a \in F$ in the basis $\vec{\alpha}$. Then each linear transformation $\psi \in \mathcal{L}$ is defined by some matrix $A(\psi) \in P_{n,n}$ such that for any $a \in F$

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

Evidently, the sequence v 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 columns of coordinates $v^\downarrow(i)$ of items $v(i)$ satisfy the relation

$$\forall i \geq 0: v^\downarrow(i+m) = A(\psi_{m-1})v^\downarrow(i+m-1) + \dots + A(\psi_0)v^\downarrow(i). \quad (2.1)$$

We call the polynomial $\mathcal{A}(x) = x^m - \sum_{j=0}^{m-1} A(\psi_j)x^j$ a *skew characteristic polynomial of LRS v in a matrix form*.

For any polynomial $\mathcal{A}(x) = x^m - \sum_{j=0}^{m-1} A_j x^j \in P_{n,n}[x]$ and any invertible matrix $L \in P_{n,n}^*$ define the polynomial

$$\mathcal{A}^L(x) = x^m - \sum_{j=0}^{m-1} L A_j L^{-1} x^j. \quad (2.2)$$

It is known [3] that $\mathcal{A}^L(x)$ is MP-polynomial if and only if $\mathcal{A}(x)$ is MP-polynomial. Define by $\mathcal{A}^{\mathcal{L}}(x)$ the set of all different polynomials of the form (2.2).

Theorem 1. *If*

$$f(x) = x^{mn} - f_{mn-1}x^{mn-1} - \dots - f_1x - f_0 \quad (2.3)$$

is a primitive polynomial of degree mn over P , then the polynomial

$$\mathcal{A}(x) = x^m - A_{m-1}x^{m-1} - \dots - A_1x - A_0, \quad (2.4)$$

where

$$A_0 = \begin{pmatrix} 0 & e & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e \\ f_0 & f_m & \dots & f_{(n-1)m} \end{pmatrix} \quad (2.5)$$

and

$$A_t = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \\ f_t & \dots & f_{(n-1)m+t} \end{pmatrix}, \quad t \in \overline{1, m-1}, \quad (2.6)$$

is a non-linearized MP-polynomial and

$$|\mathcal{A}^{\mathcal{L}}(x)| = \frac{|\mathcal{L}^*|}{|P^*|}. \quad (2.7)$$

To prove this theorem we have to use some properties of generalized multipliers, which will be defined below.

Let v be MP LRS of order m over the field F . We say that a linear transformation $\psi \in \mathcal{L}$ is (*generalized*) *multiplier* of the sequence v if

$$\psi(v) = x^l v, \quad (2.8)$$

for some $l \in \mathbb{N}$. It is known [3] that if (2.8) is true, then the transformation ψ is invertible. Let us denote by $\mathfrak{M}(v)^*$ the set of all multipliers of the sequence v . It is obvious that if $\Psi(x)$ is a characteristic polynomial of MP LRS v , then

$$|\Psi^{\mathcal{L}}(x)| = \frac{|\mathcal{L}^*|}{|\mathfrak{M}(v)^*|}. \quad (2.9)$$

From [6] we know that the set $\mathfrak{M}(v)^*$ is a cyclic subgroup of the group \mathcal{L}^* . We'll use the following definition

$$\mathfrak{M}(v) = \mathfrak{M}(v)^* \cup \{0\}.$$

Theorem 2. *The set $\mathfrak{M}(v)$ with operations of the ring \mathcal{L} is a field and up to isomorphism*

$$P < \mathfrak{M}(v) < F. \quad (2.10)$$

Theorem 3. For MP LRS v over F the following statements are equivalent:

- (a) $\mathfrak{M}(v) \cong F$;
- (b) the sequence v is linearized.

Under the condition (b), if u is a classic MP LRS over F , $\psi \in \mathcal{L}^*$ and $v = \psi(u)$, then

$$\mathfrak{M}(v) = \psi^{-1}F\psi.$$

Now in view of (2.9) and (2.10) first of all it is interesting to describe v with

$$\mathfrak{M}(v) = P. \quad (2.11)$$

If MP LRS v satisfies the condition (2.11), we say that v is *maximally non-reducible*.

Any sequence $v \in F^{(1)}$ has unique representation in the form

$$v = v_0\alpha_0 + \dots + v_{n-1}\alpha_{n-1}, \quad (2.12)$$

where $v_0, \dots, v_{n-1} \in P^{(1)}$ are *coordinate sequences* of the sequence v (in the basis $\vec{\alpha}$).

Let v be a skew MP LRS over the field F of order m . It is known [3] that sequences v_0, \dots, v_{n-1} are classic MP LRS of order mn over the field P , so for any $j \in \overline{0, n-1}$ there exists exactly one $l_j \in \overline{0, \tau-1}$ such that $v_j = x^{l_j}v_0$. We say that the set

$$l_1, \dots, l_{n-1} \quad (2.13)$$

is *determining set of shifts* of the sequence v (in the basis $\vec{\alpha}$). According to [4], v is linearized if and only if all shifts l_1, \dots, l_{n-1} are multiples of $\delta = \frac{q^{mn}-1}{q^n-1}$.

We have the following sufficient conditions.

Theorem 4. A skew MP LRS v is maximally non-reducible in each of the following cases:

- (a) In the determining set of shifts l_1, \dots, l_{n-1} of the sequence v exactly one is not a multiple of δ ;
- (b) In the determining set of shifts l_1, \dots, l_{n-1} of the sequence v exactly two are not a multiple of δ and $2 \nmid n$;

(c) The sequence v is non-linearized and n is a prime number.

Now let v be any P -skew MP LRS of order m over F .

Theorem 5. *If $\mathfrak{M}(v) \cong P' < F$, then there exists $\psi \in \mathcal{L}^*$ such that $w = \psi(v)$ is maximally non-reducible P' -skew MP LRS of order m over F .*

Theorem 6. *For any divisor s of number n and any $m \in \mathbb{N}$ there exists MP LRS v of order m over the field F such that*

$$\mathfrak{M}(v) = \text{GF}(q^s) \quad (2.14)$$

3 Proof of Theorem 2

Let θ be a root of a minimal polynomial $f(x) \in P[x]$ of the sequence v in the extension $Q = P(\theta)$ of the field P . It is known that coordinate sequences $v_s, s \in \overline{0, n-1}$, may be represented in the following way:

$$v_s(i) = \text{Tr}_P^Q(c_s \theta^i), \quad i \geq 0. \quad (3.1)$$

Let $\vec{c} = (c_0, \dots, c_{n-1})$ be the vector of determining coefficients of the sequence v .

In terms of matrices, a matrix A is a multiplier of the sequence v^\downarrow if

$$Av^\downarrow = x^l v^\downarrow \quad (3.2)$$

for some $l \geq 0$.

Lemma 7. *The condition (3.2) is equivalent to the condition*

$$(E\theta^l - A)c^\downarrow = 0, \quad (3.3)$$

where E is the identity $n \times n$ -matrix.

□ Using representation (3.1), we can rewrite the equality (3.2) as

$$A \cdot \text{Tr}_P^Q(\theta^i c^\downarrow) = \text{Tr}_P^Q(\theta^{i+l} c^\downarrow), \quad \forall i \geq 0.$$

(Here, the function Tr_P^Q applies to each coordinate of corresponding vectors.) Since Tr_P^Q is a linear transformation of the space ${}_P Q$, the last equation is equivalent to the condition

$$\text{Tr}_P^Q(\theta^i (E\theta^l - A)c^\downarrow) = 0, \quad \forall i \geq 0. \quad (3.4)$$

Now, since the condition (3.4) is true for any $i \in \mathbb{N}_0$, the condition (3.4) is equivalent to the condition (3.3). \square

If $A^{(1)}, A^{(2)} \in \mathfrak{M}(v)^*$ and $A^{(1)} \neq A^{(2)}$, then

$$(E\theta^{l_j} - A^{(j)})c^\downarrow = 0$$

for some $l_j \geq 0$, $j = 1, 2$, and therefore

$$(E(\theta^{l_1} - \theta^{l_2}) - (A^{(1)} - A^{(2)}))c^\downarrow = 0.$$

Since $A^{(1)} \neq A^{(2)}$, we have $\theta^{l_1} - \theta^{l_2} \neq 0$ and according to lemma 8 the matrix $(A^{(1)} - A^{(2)})$ is a multiplier of v . So the set $\mathfrak{M}(v)$ is closed under the addition, i.e. $\mathfrak{M}(v)$ is a field. Further, the left part of (2.10) is obvious, the right inequality follows from the fact that the maximal subfield of the ring $P_{n,n}$ has capacity $|F| = q^n$. Theorem 1 is proved.

4 Proof of Theorem 3

Consider the condition (3.3) for primitive matrix $A \in \mathfrak{M}(v)$. It is known that characteristic polynomial $\chi_A(x)$ has the form

$$\chi_A(x) = g(x)^k, \tag{4.1}$$

where $g(x)$ is irreducible polynomial.

Lemma 8. *If $k = 1$, then v is linearized.*

\square It is known [1] that there exists an invertible matrix $U \in P_{n,n}^*$ such that

$$A = U^{-1}S(g(x))U,$$

where $S(g(x))$ is the companion matrix of the polynomial $g(x)$, so

$$S(g(x)) \cdot Uc^\downarrow = \theta^l Uc^\downarrow.$$

The vector $Uc^\downarrow = (d_0, \dots, d_{n-1})^T$ is the vector of determining coefficients of the sequence $w^\downarrow = Uv^\downarrow$. Up to the shift of w we may suppose that $d_0 = e$.

So we have

$$\begin{pmatrix} 0 & 0 & \dots & 0 & g_0 \\ e & 0 & \dots & 0 & g_1 \\ 0 & e & \dots & 0 & g_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e & g_{n-1} \end{pmatrix} \begin{pmatrix} e \\ d_1 \\ d_2 \\ \dots \\ d_{n-1} \end{pmatrix} = \theta^l \begin{pmatrix} e \\ d_1 \\ d_2 \\ \dots \\ d_{n-1} \end{pmatrix},$$

therefore $g_0 d_{n-1} = \theta^l$ and for any $j \in \overline{1, n-1}$

$$d_j = \theta^{-l}(d_{j-1} + g_j d_{n-1}),$$

i.e.

$$d_j = \theta^{-l} d_{j-1} + g_j g_0^{-1}. \quad (4.2)$$

Since $d_0 = e \in F$, we have $d_0, \dots, d_{n-1} \in F^* = \{\theta^{\delta t}, t \in \overline{0, q^n - 2}\}$. Therefore all shifts in the determining set of shifts of w are multiples of δ , i.e. w is linearized and so v is linearized. \square

(a) \Rightarrow (b). Suppose that v is non-linearized, then from lemma 8 we have $k \geq 2$, therefore

$$|\mathfrak{M}(v)| = q^{\deg(g(x))} < q^n = |F|,$$

i.e. $\mathfrak{M}(v) \not\cong F^*$.

(b) \Rightarrow (a). Obvious.

Theorem 2 is proved. \square

5 Proof of Theorem 4

Let c^\downarrow be the vector of determining coefficients of the sequence v . Up to the shift of v we suppose that $c_0 = e$. Now it is evident, that $\delta \mid l_j$ if and only if $c_j \in F$.

Lemma 9. *If (3.2) is true and $\theta^l \in P$, then $A = E\theta^l$.*

\square Since the system (e, c_1, \dots, c_{n-1}) is linearly independent over P , then according to (3.3) we conclude that $E\theta^l - A = 0$. \square

(a) Suppose, for example, that $\delta \nmid l_1$, then $c_1 \notin F$. From (3.3) we obtain

$$\sum_{i \neq 1} a_{1i}c_i + a_{11}c_1 = \theta^l \cdot c_1$$

and

$$(a_{11} - \theta^l)c_1 \in F.$$

Since $\theta^l \in F$, from the last equation we have $a_{11} - \theta^l = 0$. Therefore $\theta^l \in P$ and $\mathfrak{M}(v) \subset \hat{P}$ according to lemma 9.

(b) Suppose, for example, that $\delta \nmid l_1, l_2$, then $c_1, c_2 \notin F$. Similarly to the previous case, we have:

$$a_{11}c_1 + a_{12}c_2 - \theta^l c_1 \in F,$$

$$a_{21}c_1 + a_{22}c_2 - \theta^l c_2 \in F.$$

From here

$$(a_{11} - \theta^l)(a_{22} - \theta^l) = a_{21}a_{12}.$$

If $\theta^l \notin P$, then θ^l is the root of the polynomial over P of degree 2, and therefore $2|n$. So $\theta^l \in P$ and similarly to the previous case $\mathfrak{M}(v) = \hat{P}$.

The statement (c) follows from theorem 2 and theorem 3.

6 Proof of Theorem 5

If the matrix A in the equality (3.2) generates $\mathfrak{M}(v)^*$, then $\mathfrak{M}(v) \cong P(\theta^l)$. Fix basis $\vec{\alpha}$ of the space ${}_P F$ of the form

$$\vec{\alpha} = \vec{\gamma} \otimes \vec{\beta},$$

where $\vec{\gamma} = (\gamma_0, \dots, \gamma_{s-1})$ is the basis of the space ${}_P P(\theta^l)$ and $\vec{\beta} = (\beta_0, \dots, \beta_{k-1})$ is the basis of the space ${}_P(\theta^l) F$.

It is known that the matrix A has the second normal form

$$N_2(A) = E_k \otimes S(g(x)) = \text{Diag}(S(g(x)), S(g(x)), \dots, S(g(x))). \quad (6.1)$$

Further, as in the proof of the lemma 9, there exists $\psi \in \mathcal{L}^*$ such that the vector of determining coefficients of the sequence $w = \psi(v)$ has the form

$$\vec{c} = (d_0 \vec{c}_*, d_1 \vec{c}_*, \dots, d_{k-1} \vec{c}_*), \quad (6.2)$$

where $\vec{c}_* \in P(b)^s$ and $\vec{d} = (d_0, d_1, \dots, d_{k-1}) \in Q^k$.

Note that in this case the vector $\vec{c}_* \in (P(\theta^l))^s$ is the vector of determining coefficients of some linearized P -skew MP LRS u of order ms over $P(\theta^l)$, so we can choose ψ such that u will be a classic P -skew MP LRS over $P(\theta^l)$. Now

$$w = (x^{\Delta_0}\beta_0 + \dots + x^{\Delta_{k-1}}\beta_{k-1})(\gamma_0u_0 + \dots + \gamma_{s-1}u_{s-1}) = (x^{\Delta_0}\beta_0 + \dots + x^{\Delta_{k-1}}\beta_{k-1})u,$$

where $\theta^{\Delta_t} = d_t$, $t \in \overline{0, k-1}$. So the sequence w is $P(\theta^l)$ -skew MP LRS of order m over F , and $\mathfrak{M}(w) = P(\theta^l)$.

7 Proof of Theorem 6

Let w be a maximally non-reducible K -skew MP LRS of order m over F (the existence of such sequences follows, for example, from theorem 7). From the proof of theorem 5 it is evident that w is also P -skew MP LRS of order m over F and $\mathfrak{M}(w) \cong K$.

8 Proof of Theorem 1

□ Let v be a MP LRS with the vector of determining coefficients

$$\vec{c} = (e, \theta^m, \dots, \theta^{(n-1)m}). \quad (8.1)$$

Since the system

$$\vec{\theta} = (\vec{c}, \theta\vec{c}, \dots, \theta^{m-1}\vec{c}) = \quad (8.2)$$

$$= (e, \theta^m, \dots, \theta^{m(n-1)}, \theta, \theta^{m+1}, \dots, \theta^{m(n-1)+1}, \dots, \theta^{m-1}, \theta^{2m-1}, \dots, \theta^{mn-1})$$

is a basis of the space ${}_PQ$, according to [3] v is a skew MP LRS.

It is easy to see that the matrix

$$B = \begin{pmatrix} & \mathbb{O} & & E & & \dots & & \mathbb{O} & & & & \\ & \vdots & & \vdots & & \ddots & & \vdots & & & & \\ & \mathbb{O} & & \mathbb{O} & & \dots & & E & & & & \\ 0 & e & \dots & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & e & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \\ F_0 & F_m & \dots & F_{(n-1)m} & F_1 & \dots & F_{(n-1)m+1} & \dots & F_{m-1} & \dots & F_{mn-1} & \end{pmatrix} \quad (8.3)$$

satisfies the following equality:

$$B\theta^\downarrow = \theta\theta^\downarrow.$$

So we define matrices A_0, \dots, A_{m-1} as successive n rows of the matrix B by the equality

$$(A_0, \dots, A_{m-1}) = \begin{pmatrix} \vec{B}_{(m-1)n+1} \\ \dots \\ \vec{B}_{mn} \end{pmatrix}. \quad (8.4)$$

Then [3]

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

is a skew MP-polynomial in a matrix form.

To prove the last equality we have to prove that v is maximally non-reducible MP LRS. Suppose $A \in \mathfrak{M}(v)$, then equation (3.3) may be represented as

$$(E\theta^l - A) \begin{pmatrix} e \\ \theta^m \\ \vdots \\ \theta^{(n-1)m} \end{pmatrix} = 0.$$

For $s \in \overline{0, n-1}$ the following equalities are true

$$\sum_{j=0}^{n-1} a_{sj} \theta^{mj} = \theta^l \theta^{sm},$$

therefore,

$$\sum_{j=0}^{n-1} a_{sj} \theta^{m(j+1)} = \sum_{j=0}^{n-1} a_{s+1,j} \theta^{mj}$$

or

$$a_{s,n-1} \theta^{mn} + \sum_{j=1}^{n-1} (a_{s,j-1} - a_{s+1,j}) \theta^{mj} + a_{s+1,0} = 0.$$

So, the element θ is annihilated by a polynomial of the form $h(x^m)$, but from [1] we know that there are no MP-polynomials of the form $h(x^m)$. Therefore

$$a_{s,n-1} = a_{s+1,0} = a_{s0} - a_{s+1,1} = \dots = a_{s,n-2} - a_{s+1,n-1} = 0. \quad (8.5)$$

From (8.5) we obtain that for any $s, j \in \overline{0, n-2}$

$$a_{sj} = a_{s+1,j+1}, \quad a_{s,n-1} = 0, \quad a_{s+1,0} = 0,$$

and this means that the matrix A is a scalar one.

The theorem 1 is proved.

References

- [1] *Glukhov M. M., Elizarov V. P., Nechaev A. A.* Algebra, Volume 2. — Moscow: Gelios ARV, 2003.
- [2] *Kuzmin A. S., Kurakin V. L., Nechaev A. A.* Galois rings as application to the codes and linear recurrences // in press.
- [3] *Goltvanitsa M. A., Zaitsev S. N., Nechaev A. A.* Skew linear recurrences of maximal period over Galois rings // Fundamental and applied mathematics. — 2011/2012. — V. 17, №3. — P. 5–23.
- [4] *Goltvanitsa M. A., Zaitsev S. N., Nechaev A. A.* Skew LRS of maximal period over Galois rings // Workshop on Current Trends in Cryptology, 2012.
- [5] *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over ring and modules // J. Math. Sci. — 1995. — V. 76. No 6. — P. 2793–2915.

-
- [6] *Nechaev A. A., Kuzmin A. S., Kurakin V. L.* Structural, analytical and statistical properties of linear and polylinear recurrent sequences // Tr. Diskr. Mat., vol. 3 — Moscow: FIZMATLIT, 2000. — P. 155–194.
- [7] *Kurakin V. L.* Berlekamp-Massey algorithm over finite rings, modules and bimodules // Discrete mathematics. — 1998. — V. 10. No 4. — P. 3–34.
- [8] *Nechaev A. A.* Finite rings with applications // Handbook of Algebra, vol. 5, edited by M. Hazewinkel — Elsevier B.V. — 2008. — P. 213–320.
- [9] *Nechaev A. A.* Finite rings of principal ideals // Mat. USSR-Sb. — 1973. — V. 20. No 3. — P. 364–382.
- [10] *McDonald B. R.* Finite rings with identity. — New York: Markel Dekker, 1974.
- [11] *Lidl R., Niederreiter H.* Finite fields. — Cambridge University Press, 1983.
- [12] *Nechaev A. A.* Kerdock's code in cyclic form // Discrete Math. Appl. — 1991. — V. 1. No 4. — P. 365–384.
- [13] *Nechaev A. A.* Linear recurrent sequences over commutative rings // Discrete Math. Appl. — 1992. — V. 2. No 6. — P. 659–683.
- [14] *Nechaev A. A.* Cycle types of linear substitutions over finite commutative rings // Russian Acad. Sci. Sb. Math. — 1994. — V. 78. No 2. — P. 283–311.
- [15] *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules // Journal of Mathematical Sciences. — 1995. — V. 76. No 6. — P. 2793–2915.
- [16] *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. — Vol. 102. No. 6. — 2000. — P. 4598–4626.

- [17] *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.
- [18] *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>.
- [19] *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.
- [20] *Zeng G., Yang Y., Han W., Fan S.* Word oriented cascade jump σ -LFSR // *AAECC 2009, LNCS.* — 2009. — V. 5527. — P. 127–136.
- [21] *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.
- [22] *Ghorpade S. R., Ram S.* Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields // *Finite Fields and Their Appl.* — 2011. — Vol. 17. No. 5. — P. 461–472.