Math-Net.Ru

Общероссийский математический портал

М. А. Goltvanitsa, Построение скрученных ЛРП максимального периода над конечными полями с помощью определяющих наборов коэффициентов, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 2, 37–46

DOI: <https://doi.org/10.4213/mvk115>

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: 52.23.180.231

26 апреля 2023 г., 13:31:48

A construction of skew LRS of maximal period over finite fields based on the defining tuples of factors

M. A. Goltvanitsa

LLC "Certification Research Center", Moscow

Received 25.09.2013

Let p be a prime number, $R = \text{GF}(q)$ be a field of $q = p^r$ elements and $S = \text{GF}(q^n)$ be an extension of R . Let $\check{S}$ be the ring of all linear transformations of the space ${}_R S$. A linear recurrent sequence v of order m over the module ${}_S S$ is said to be a *skew linear recurrence sequence (skew LRS) of order m over S* . The period $T(v)$ of such sequence satisfies the inequality $T(v) \leq \tau = q^{mn} - 1$. If $T(v) = \tau$ we call v a *skew LRS of maximal period (skew MP LRS)*. Here new classes of skew MP LRS based on the notion of *the defining tuples of factors* are constructed.

Keywords: finite field, skew linear recurrence of maximal period.

Построение скрученных ЛРП максимального периода над конечными полями с помощью определяющих наборов коэффициентов

М. А. Гольтованица

ООО "Центр сертификационных исследований", г. Москва

Аннотация. Пусть p — простое число, $R = \text{GF}(q)$ — поле из $q = p^r$ элементов и $S = \text{GF}(q^n)$ — расширение R . Пусть $\check{S}$ — кольцо всех линейных преобразований пространства ${}_R S$. Линейная рекуррентная последовательность v порядка m над модулем ${}_S S$ называется *скрученной линейной рекуррентной последовательностью (скрученной LRS) порядка m над S* . Период $T(v)$ такой последовательности удовлетворяет неравенству $T(v) \leq \tau = q^{mn} - 1$. Если $T(v) = \tau$, то мы называем v *скрученной ЛРП максимального периода (скрученной МП ЛРП)*. Здесь с помощью *определяющих наборов коэффициентов* построены новые классы скрученных МП ЛРП.

Ключевые слова: конечные поля, скрученные линейные рекурренты, максимальный период.

1 Introduction. Preliminaries

Below $R = \text{GF}(q)$ is a Galois field with identity e , $q = p^r$, $p = \text{char} R$, $S = \text{GF}(q^n)$, $n \geq 2$, is an extension of R [3]. Denote by S^* multiplicative group of S . Let σ be a generator of the group $\text{Aut}(S/R)$ of automorphisms of S over R . Then $\text{ord } \sigma = n$. Let $\check{S} = S^\sigma \langle \sigma \rangle$ be a ring 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 multiplication, defined by distributivity from the identity $\sigma s = \sigma(s)\sigma$, $s \in S$.

Each element $\psi \in \check{S}$ defines a linear transformation of the space ${}_R S$ such that $\psi(s) = \sum_{i=0}^{n-1} s_i \sigma^i(s)$ for every $s \in S$.

Let us set a structure of a left $\check{S}[x]$ -module on the set $S^{(1)}$ of all sequences over S by introducing the product of a sequence $v \in S^{(1)}$ and a polynomial $A(x) = \sum_{i \geq 0} a_i x^i \in \check{S}[x]$ by the equality

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

So the structure of a left $\check{S}[x]$ -module on $S^{(1)}$ is given. We say that $v \in S^{(1)}$ is a *skew linear recurrent sequence (LRS)* of order m over S , if it is LRS of order m over the module ${}_S \check{S}$ [4], i.e. $\Psi(x)v = 0$ for some monic polynomial $\Psi(x) = x^m - \sum_{j=0}^{m-1} \psi_j x^j \in \check{S}[x]$, called *skew characteristic polynomial of LRS v* , that is $v(i+m) = \sum_{j=0}^{m-1} \psi_j (v(i+j))$ for all $i \in \mathbb{N}_0$. By $L_S(\Psi)$ we denote the set of all skew LRS over S with characteristic polynomial Ψ .

It was shown in [1] that 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 with the property $L_S(\Psi) \subset L_S(F)$. So, a period of any skew LRS $v \in L_S(\Psi)$ satisfies the following relations: $T(v)|T(F)$, $T(F) \leq \tau = q^{nm} - 1$. If $T(v) = \tau$, then we say that v is a skew LRS of *maximal period (MP LRS)* and $\Psi(x)$ is a *skew MP-polynomial*. Skew MP LRS were studied earlier in works [1], [2], [4], [6]–[11].

Below we use the notation $v[\overline{i, i+t}] = (v(i), v(i+1), \dots, v(i+t))$ for $i, t \in \mathbb{N}_0$.

Theorem 1. ([1]). *A sequence $v \in S^{(1)}$ is a skew MP LRS of order m if and only if $v[\overline{i, i+m-1}] \neq (0, 0, \dots, 0)$ for all $i \in \mathbb{N}_0$ and there exists an MP-polynomial $F(x) \in R[x]$ of degree mn such that $v \in L_S(F)$.*

The following result gives the first explicit method permitting to construct a class of skew MP-polynomials from one skew MP-polynomial.

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

Under the conditions of Theorem 2, if v is a classic MP LRS, that is if $\Psi(x) \in S[x]$, we say that a skew MP LRS $w = \psi(v)$ and the polynomial $\Psi'(x) \in \check{S}[x]$ are *linearized*. The class of linearized MP-polynomials was described in [1]. In [2] new classes of skew non-linearized MP-polynomials over Galois rings were constructed.

Here a new approach to the construction of the skew MP LRS over fields is proposed. Under the notations of Theorem 1 let θ be a root of the polynomial $F(x)$ in the extension $K = \text{GF}(q^{mn})$ of the field S . Then $F(x)$ has a canonical decomposition over S :

$$F(x) = F_0(x) \cdot \dots \cdot F_{n-1}(x), \quad F_j(\theta_j) = 0, \theta_j = \theta^{q^j}, \quad j = 0, 1, \dots, n-1,$$

where $F_0(x), \dots, F_{n-1}(x)$ are MP-polynomials of degree m over S [3]. Therefore, every $v \in L_S(F)$ has a unique representation $v = w_0 + \dots + w_{n-1}$, where $w_j \in L_S(F_j)$. Let tr_S^K be a trace function from the field K onto the field S [3]. Then for every $j \in \overline{0, n-1}$ there exists a unique element $\varepsilon_j \in K$ such that $w_j(i) = \text{tr}_S^K(\varepsilon_j \theta_j^i)$, $i \geq 0$ [5]. The tuple

$$(\varepsilon_0, \dots, \varepsilon_{n-1}) \tag{1}$$

is called *the defining tuple of factors* of LRS v . The following result describes a construction of the defining tuples of factors of the skew linearized MP LRS.

Theorem 3. *A sequence $v \in L_S(F)$ with the defining tuple of factors (1) is a skew linearized MP LRS of order m iff there exists an element $\beta \in K^*$ and an invertible transformation $\varphi = \sum_{j=0}^{n-1} b_j \sigma^j \in \check{S}^*$ such that $\varepsilon_j = b_j \beta^{q^j}$ for every $j \in \overline{0, n-1}$.*

Let us show how to construct new classes of skew non-linearized MP LRS by means of their defining tuples of factors. The automorphism $\sigma \in \check{S}$ may be extended to automorphism of the field K over R by the natural way $\sigma(\varkappa) = \varkappa^q$, $\varkappa \in K$. So to every elements $\varkappa_0, \dots, \varkappa_{n-1} \in K$ there corresponds a linear transform

$$\chi = \varkappa_0 + \varkappa_1 \sigma + \dots + \varkappa_{n-1} \sigma^{n-1} : K \rightarrow K \tag{2}$$

such that $\chi(\varkappa) = \sum_{j=0}^{n-1} \varkappa_j \sigma^j(\varkappa)$ for every $\varkappa \in K$. Let the system $(\alpha_0, \dots, \alpha_{n-1})$ be a basis of the space ${}_R S$.

Lemma 4. *For every elements $\beta_0, \dots, \beta_{n-1} \in K$ there exists a unique map $\chi = \sum_{j=0}^{n-1} \varkappa_j \sigma^j$ such that $\chi(\alpha_j) = \beta_j$, $j = 0, 1, \dots, n-1$.*

In the proof of Lemma 4 the constructive algorithm for determining the elements $\varkappa_0, \dots, \varkappa_{n-1}$ of transform χ will be presented.

Using Lemma 4, we can determine the elements $\varkappa_0, \dots, \varkappa_{n-1}$ of transform (2) by fixing the elements $\chi(\alpha_0), \dots, \chi(\alpha_{n-1}) \in K$ and sometimes it is very convenient. Let us put $m \geq 2$, $\xi = \theta^{q^{n-1}}$ and $h = (-e)^{m-1} \xi^{-\frac{q^{mn-1}}{q^n-1}}$.

Theorem 5. Let $\vec{\beta} = (\beta_0, \dots, \beta_{n-1})$ be an arbitrary basis of the space ${}_R S$. Let $k \in \overline{1, n-1}$ be fixed, for any $w_0, \dots, w_{k-1} \in {}_R(\beta_0, \dots, \beta_{k-1})$ we define elements $\varkappa_0, \dots, \varkappa_{n-1}$ of map (2) by conditions

$$\chi(\alpha_j) = \beta_j, j = 0, 1, \dots, k-1; \quad \chi(\alpha_j) = \beta_j h\xi + w_{j-k}, j = k, k+1, \dots, n-1. \quad (3)$$

Then the sequence $v \in L_S(F)$ with the defining tuple of factors

$$(\varkappa_{n-1}^q, \varkappa_{n-2}^{q^2}, \dots, \varkappa_0)$$

is a skew non-linearized MP LRS of order m over S .

Using Theorem 5 we can construct a number of skew non-linearized MP LRS. But this Theorem doesn't give information about skew characteristic polynomials of these sequences. So, this question is open. To find the skew characteristic polynomial of concrete skew MP LRS we can apply the Berlekamp-Massey algorithm for modules developed by Kurakin V.L. in [12].

1.1 Cryptographic applications

Any skew MP LRS may be considered as a pseudo-random sequence. It was shown in [1] that a linear complexity of skew MP LRS as LRS over field S may be greater than a linear complexity of classic LRS.

2 Proofs

2.1 Proof of Theorem 3

Let $v \in L_S(F)$ be a linearized skew MP LRS of order m with the defining tuple of factors (1). Then for some $k \in \overline{0, n-1}$ there exists an invertible transform $\psi = \sum_{j=0}^{n-1} c_j \sigma^j$ and an element $\varkappa \in K^*$ such that

$$v(i) = \psi(\text{tr}_S^K(\varkappa \theta_k^i)) = (\psi \cdot \sigma^k)(\text{tr}_S^K(\varkappa^{q^{mn-k}} \theta^i)) \quad \forall i \in \mathbb{N}_0.$$

Then $\varphi = (\psi \cdot \sigma^k) = \sum_{j=0}^{n-1} b_j \sigma^j$ for some $b_0, \dots, b_{n-1} \in S$. Evidently, this φ is an invertible transform of the space ${}_R S$. So, $v(i) = \sum_{j=0}^{n-1} \text{tr}_S^K(b_j \beta^{q^j} \theta^{q^j i})$ for $\beta = \varkappa^{q^{mn-k}}$. Now the sufficiency follows from the chain of equalities $v(i) = \sum_{j=0}^{n-1} \text{tr}_S^K(b_j \beta^{q^j} \theta^{q^j i}) = \sum_{j=0}^{n-1} b_j \sigma^j(\text{tr}_S^K(\beta \theta^i)) = \varphi(\text{tr}_S^K(\beta \theta^i))$.

2.2 Proof of Lemma 4

Let $S_{n,n}$ be a ring of all $n \times n$ matrices over S and let $A = (a_{ij})_{i,j=1}^n \in S_{n,n}$ be a matrix such that $a_{ij} = \alpha_{i-1}^{q^{j-1}}$. Let $Y^\downarrow = (\beta_0, \dots, \beta_{n-1})^T$, then the column $(\varkappa_0, \dots, \varkappa_{n-1})^T$ satisfies the system of linear equations $AX^\downarrow = Y^\downarrow$ over K . Since $(\alpha_0, \dots, \alpha_{n-1})$ is a linearly independent system over R , we have A is an invertible matrix over S [3]. Then $(\varkappa_0, \dots, \varkappa_{n-1})^T = A^{-1}Y^\downarrow$.

2.3 Proof of Theorem 5

Let $S[x|m]$ be the set of all polynomials over S of degree less than m . The following characterization of skew MP LRS in terms of the defining tuples of factors is obtained.

Lemma 6. *The sequence $v \in L_S(F)$ with the defining tuple of factors (1) is a skew MP LRS of order m iff for every polynomial $c(x) \in S[x|m] \setminus \{0\}$ the following condition is fulfilled*

$$\varepsilon_{n-1}c(\theta^{q^{n-1}}) + (\varepsilon_{n-2}c(\theta^{q^{n-2}}))^q + \dots + (\varepsilon_0c(\theta))^{\theta^{n-1}} \neq 0. \quad (4)$$

□ Let R_0 be a prime subfield [3] of the field R and $\chi : (S, +) \rightarrow (C^*, \cdot)$ be a canonical additive character of the field S [3], i.e. $\chi(z) = \exp \left\{ \frac{2\pi i}{p} \text{tr}_{R_0}^S(z) \right\}$ for every $z \in S$. Let us put $N = |\{i \in \overline{0, q^{mn} - 2} : v[i, i+m-1] = (0, 0, \dots, 0)\}|$. Then by Theorem 1 v is a skew MP LRS iff $N = 0$. Using the well-known properties of characters [3], we get

$$N = \sum_{i=0}^{q^{mn}-2} \left(\frac{1}{|S|} \sum_{c_0 \in S} \chi(c_0 v(i)) \right) \left(\frac{1}{|S|} \sum_{c_1 \in S} \chi(c_1 v(i+1)) \right) \times \dots \\ \dots \times \left(\frac{1}{|S|} \sum_{c_{m-1} \in S} \chi(c_{m-1} v(i+m-1)) \right). \quad (5)$$

Now on interchanging the order of summation in (5), we have

$$N = \frac{1}{q^{mn}} \sum_{c_0 \in S} \dots \sum_{c_{m-1} \in S} \sum_{i=0}^{q^{mn}-2} \chi \left(\sum_{j=0}^{m-1} c_j v(i+j) \right) = \\ = \frac{1}{q^{mn}} \sum_{c(x) \in S[x|m]} \sum_{i=0}^{q^{mn}-2} \chi(c(x)v(i)). \quad (6)$$

Since $c(x)v(i) = \text{tr}_S^K \left(\sum_{j=0}^{n-1} \varepsilon_j c(\theta^{q^j}) \theta^{q^j i} \right)$, we obtain

$$N = \frac{1}{q^{mn}} \sum_{c(x) \in S[x|m]} \sum_{i=0}^{q^{mn}-2} \chi \left(\text{tr}_S^K \left(\sum_{j=0}^{n-1} \varepsilon_j c(\theta^{q^j}) \theta^{q^j i} \right) \right).$$

For every $j \in \overline{0, n-1}$ we have $\{\theta^{q^j i} : i \in \overline{0, q^{mn} - 2}\} = K^*$, therefore,

$$N = \frac{1}{q^{mn}} \sum_{c(x) \in S[x|m]} \sum_{y \in K^*} \chi \left(\text{tr}_S^K \left(\sum_{j=0}^{n-1} \varepsilon_j c(\theta^{q^j}) y^{q^j} \right) \right) = \\ = \frac{1}{q^{mn}} \sum_{c(x) \in S[x|m]} \sum_{y \in K^*} \hat{\chi} \left(\sum_{j=0}^{n-1} \varepsilon_j c(\theta^{q^j}) y^{q^j} \right),$$

where $\widehat{\chi} : (K; +) \rightarrow (C^*, \cdot)$ is the canonical additive character of the field K . Let $H_c(z)$ be a linearized polynomial [3] of the form $H_c(z) = \sum_{j=0}^{n-1} \varepsilon_j c(\theta^{q^j}) z^{q^j}$. Then we have

$$N = \frac{1}{q^{mn}} \sum_{c(x) \in S[x|m] \setminus \{0\}} \sum_{y \in K} \widehat{\chi}(H_c(y)).$$

Let us note that the inner sum of the last formula is the Weil sum of the special form.

Theorem 7. ([3]). *Let $F = GF(q)$, $\text{char} F = p$, and $f(x) = \sum_{j=0}^r a_j x^{p^j} + a$ be an arbitrary affine p -polynomial over F . Then for every non-trivial additive character χ_b , $b \in F^*$, of the field F the following relation is true:*

$$\sum_{c \in F} \chi_b(f(c)) = \begin{cases} \chi_b(a)q, & \text{if } ba_r + b^p a_{r-1}^p + \dots + b^{p^{r-1}} a_1^{p^{r-1}} + b^{p^r} a_0^{p^r} = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Application of Theorem 7 to the case $b = 1$ yields the requiring result. This completes the proof of Lemma 6. $\square$

Let $v \in L_S(F)$ be a sequence with the defining tuple of factors (1) and $\zeta : K \rightarrow K$ be a transform of the form

$$\zeta = \varepsilon_{n-1} + \varepsilon_{n-2}^q \sigma + \dots + \varepsilon_0^{q^{n-1}} \sigma^{n-1}. \quad (7)$$

Let $\widetilde{\zeta}$ be a restriction of transform (7) on S , i.e.

$$\widetilde{\zeta} = \zeta|_S : S \rightarrow \zeta(S) \subset K. \quad (8)$$

Lemma 8. *Let $v \in L_S(F)$ be a sequence with the defining tuple of factors (1). Then*

1. *if v is a skew MP LRS of order m , then the transform (8) is an injective one;*
2. *the sequence v is a skew linearized MP LRS of order m iff*

$$\widetilde{\zeta}(S) = \varkappa S \quad (9)$$

for some $\varkappa \in K^$.*

Proof. It is easy to see that condition (4) may be written in the following form

$$\sum_{j=0}^{m-1} \xi^j (\varepsilon_{n-1} c_j + \varepsilon_{n-2}^q c_j^q + \dots + \varepsilon_0^{q^{n-1}} c_j^{q^{n-1}}) = \sum_{j=0}^{m-1} \zeta(c_j) \xi^j \neq 0. \quad (10)$$

Assume that transform (8) is not injective one, then there exists $c_0 \in S^*$ such that $\zeta(c_0) = 0$. Then for the polynomial $c(x) = c_0 \in S[x|m] \setminus \{0\}$ condition (10) is not fulfilled. Therefore, v is not a skew MP LRS of order m , what is a contradiction.

Let us prove the second item. For every $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in S^n$ we put

$$C^\sigma(\vec{a}) = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ \sigma(a_{n-1}) & \sigma(a_0) & \dots & \sigma(a_{n-2}) \\ \vdots & \ddots & \ddots & \vdots \\ \sigma^{n-1}(a_1) & \sigma^{n-1}(a_2) & \dots & \sigma^{n-1}(a_0) \end{pmatrix}.$$

Lemma 9. *The set $C^\sigma(S) = \{C^\sigma(\vec{a}) : \vec{a} \in S^n\}$ is a subring in $S_{n,n}$, moreover, $C^\sigma(S) \cong \check{S}$.*

□ For every element $a \in S$ let us put $D(a) = \text{diag}(a, \sigma(a), \dots, \sigma^{n-1}(a))$. Since σ is automorphism, we obtain that the set $\{D(a) : a \in S\}$ is a subring in $S_{n,n}$. Let T be a matrix of the following form $T = (t_{ij})_{i,j=1}^n$, $t_{ij} = e\delta_{(j-i) \bmod n, 1}$, where $\delta_{i,j}$ is the Kronecker delta. For an arbitrary vector $\vec{a} = (a_0, a_1, \dots, a_{n-1}) \in S^n$ the following equality is valid

$$C^\sigma(\vec{a}) = D(a_0)T^0 + D(a_1)T + \dots + D(a_{n-1})T^{n-1}.$$

The set $C^\sigma(S)$ is closed under the additive operation in the ring $S_{n,n}$. Let us show the closure of $C^\sigma(S)$ under the matrix product operation. Let $C^\sigma(\vec{a}), C^\sigma(\vec{b})$ be matrices of the following form $C^\sigma(\vec{a}) = \sum_{j=0}^{n-1} D(a_j)T^j$, $C^\sigma(\vec{b}) = \sum_{j=0}^{n-1} D(b_j)T^j$. Since for all $a \in S, l \in \overline{0, n-1}$ the equation $T^l D(a) = D(\sigma^l(a))T^l$ is valid, we obtain

$$C^\sigma(\vec{a})C^\sigma(\vec{b}) = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} D(a_j)D(\sigma^j(b_k))T^{j+k} = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} D(a_j\sigma^j(b_k))T^{j+k}.$$

Let $\ominus$ denote the subtraction modulo n and $c_j = \sum_{l=0}^{n-1} a_l \sigma^l(b_{j \ominus l})$, for all $j = 0, \dots, n-1$, then

$$C^\sigma(\vec{a})C^\sigma(\vec{b}) = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} D(a_j\sigma^j(b_k))T^{j+k} = \sum_{j=0}^{n-1} D(c_j)T^j. \quad (11)$$

So, $C^\sigma(S)$ is a subring of the ring $S_{n,n}$. Let the map $\Xi : \check{S} \rightarrow C^\sigma(S)$ transforms each $\sum_{j=0}^{n-1} s_j \sigma^j$ into $C^\sigma(s_0, \dots, s_{n-1})$. Evidently, Ξ is an additive bijective homomorphism.

Using (11) and the formulas for elements c_j , we obtain that Ξ is a multiplicative homomorphism. So, Ξ is an isomorphism and Lemma 9 is proved. □

Let us prove a necessity. Since v is a linearized skew MP LRS, by means Theorem 3 we obtain that there exist an invertible linear transform $\varphi = \sum_{j=0}^{n-1} b_j \sigma^j : S \rightarrow S$ and an element $\beta \in K^*$ such that $\varepsilon_j = b_j \beta^{q^j}$ for $j = 0, 1, \dots, n-1$. We have $\tilde{\zeta} = \sum_{j=0}^{n-1} \varepsilon_{n-1-j}^{q^j} \sigma^j = \beta^{q^{n-1}} \cdot \psi$, where $\psi = b_{n-1} + b_{n-2}^q \sigma + \dots + b_0^{q^{n-1}} \sigma^{n-1}$. Therefore,

$$\tilde{\zeta}(S) = \beta^{q^{n-1}} \cdot \psi(S). \quad (12)$$

Let us show that ψ is an invertible transform. By Lemma 9 it is sufficient to prove that the matrix $C^\sigma(b_{n-1}, b_{n-2}^q, \dots, b_0^{q^{n-1}})$ is an invertible one. Since φ is an invertible transform, we obtain that the matrix $C^\sigma(b_0, b_1, \dots, b_{n-1})$ is an invertible one. It is easily to see that the matrix $C^\sigma(b_{n-1}, b_{n-2}^q, \dots, b_0^{q^{n-1}})$ may be obtained from the invertible matrix $C^\sigma(b_0, b_1, \dots, b_{n-1})$ by consecutive operation of transposing and of cyclic downward shift of rows. So, for $\varkappa = \beta^{q^{n-1}}$, using (12), we obtain $\tilde{\zeta}(S) = \varkappa \cdot \psi(S) = \varkappa S$.

Let us prove the sufficiency. Under the condition $\tilde{\zeta}(S) = \varkappa S$ there exists an invertible transform $\varphi = \sum_{j=0}^{n-1} b_j \sigma^j : S \rightarrow S$ such that $\varphi(a) = \varkappa^{-1} \tilde{\zeta}(a)$ for all $a \in S$. Therefore, a polynomial of the form $\sum_{j=0}^{n-1} (b_j - \frac{\varepsilon_{n-1-j}^{q^j}}{\varkappa}) x^{q^j}$ of degree less than q^n has at least q^n different roots in the field K . Thus, we have

$$\varepsilon_j = (\varkappa b_{n-1-j})^{q^{mn-(n-1-j)}} = (\varkappa)^{q^{mn-(n-1-j)}} b_{n-1-j}^{q^{j+1}}, j = 0, 1, \dots, n-1. \quad (13)$$

Let $\zeta = b_{n-1}^q + b_{n-2}^{q^2} \sigma + \dots + b_1^{q^{n-1}} \sigma^{n-2} + b_0 \sigma^{n-1} : S \rightarrow S$. By (13) we obtain that the i -th term $v(i)$ of the sequence v has the form $v(i) = \zeta(\text{tr}_S^K(\varkappa^{q^{mn-(n-1)}} \theta^i))$. Let us show that the transform ζ is an invertible one. Since the transform $\varphi = \sum_{j=0}^{n-1} b_j \sigma^j$ is invertible, we

obtain that $C^\sigma(b_0, b_1, \dots, b_{n-1})$ is an invertible matrix. The transform ζ is invertible iff $C^\sigma(b_{n-1}^q, b_{n-2}^{q^2}, \dots, b_0)$ is an invertible matrix. Let us note that matrix $C^\sigma(b_{n-1}^q, b_{n-2}^{q^2}, \dots, b_0)$ may be obtained from the invertible matrix $C^\sigma(b_0, b_1, \dots, b_{n-1})$ by consecutive operation of transposing and left cyclic shift of columns. This completes the proof of Lemma 8. $\square$

Lemma 10. *Under the conditions of Lemma 8*

1. *if v is a linearized skew MP LRS of order m , then $\tilde{\zeta}(S) \cap S \in \{0, S\}$;*
2. *if condition (4) is fulfilled for all $c(x) \in S[x|m] \setminus \{0\}$ and*

$$0 < \dim_R(\tilde{\zeta}(S) \cap S) < n,$$

then v is non-linearized skew MP LRS of order m .

$\square$ By Lemma 8 the case $\tilde{\zeta}(S) \cap S = S$ corresponds to the case $\varkappa \in S^*$ in condition (9). If $\varkappa \in K \setminus S$, then $\tilde{\zeta}(S) \cap S = 0$. The validity of the second item of this Lemma follows from the first one and from Theorem 6. $\square$

For the skew LRS v with the defining tuple of factors $(\varkappa_{n-1}^q, \varkappa_{n-2}^{q^2}, \dots, \varkappa_0)$ the map χ in (7) is equal to the map ζ in (2). Let $\gamma_{j-k} = \beta_j h, j = k, k+1, \dots, n-1$, and $W = {}_R(\beta_0, \dots, \beta_{k-1})$. Now by (3) we obtain the following decomposition of the space $\zeta({}_R S)$:

$$\zeta({}_R S) = {}_R W \dot{+} {}_R(\zeta(\alpha_k)) \dot{+} \dots \dot{+} {}_R(\zeta(\alpha_{n-1})).$$

Let $\zeta(c_j) = \eta_j$ and $c(x) = \sum_{j=0}^{m-1} c_j x^j \in S[x|m] \setminus \{0\}$ be an arbitrary polynomial. Therefore, we have

$$\eta_j = \tilde{w}_j + b_{j0}(\gamma_0 \xi + w_0) + \dots + b_{j,n-1-k}(\gamma_{n-1-k} \xi + w_{n-1-k})$$

for some $\tilde{w}_j \in W$, $b_{js} \in R$, $j = 0, 1, \dots, n-1$, $s = 0, 1, \dots, n-1-k$. Since W is a subspace of the space ${}_R S$, we obtain

$$\eta_j = \hat{w}_j + \xi \sum_{s=0}^{n-1-k} b_{js} \gamma_s, \quad j = 0, \dots, n-1 \quad (14)$$

for some $\hat{w}_j \in W$. Under condition (14) we rewrite condition (10) in the form

$$\sum_{j=0}^{m-1} \zeta(c_j) \xi^j = \sum_{j=0}^{m-1} \hat{w}_j \xi^j + \sum_{s=0}^{n-1-k} \gamma_s \xi \sum_{j=0}^{m-1} b_{js} \xi^j \neq 0. \quad (15)$$

Let us consider two cases. If $b_{m-1,s} = 0$ for all $s \in \overline{0, n-1-k}$, then in the left side of (15) we have a value of the nonzero polynomial over S of degree less than m on the element ξ . Since the degree of minimal polynomial of ξ over S is equal to m , we obtain that condition (15) is fulfilled.

Let us consider the case

$$(b_{m-1,0}, \dots, b_{m-1,n-1-k}) \neq (0, \dots, 0). \quad (16)$$

The minimal polynomial of the element ξ over S is equal to $F_{n-1}(x)$ from the canonical decomposition of $F(x)$ over S . Let $F_{n-1}(x) = x^m - \sum_{j=0}^{m-1} h_j x^j$, therefore, $h_0 = (-e)^{m-1} \left(\xi^{\frac{q^{mn}-1}{q^n-1}} \right)$ and $h_0 = h^{-1}$. Then we can write condition (15) in the form

$$\sum_{j=0}^{m-1} \hat{w}_j \xi^j + \sum_{s=0}^{n-1-k} \gamma_s \sum_{j=1}^{m-1} b_{j-1,s} \xi^j + \left(\sum_{s=0}^{n-1-k} \gamma_s b_{m-1,s} \right) \left(\sum_{j=0}^{m-1} h_j \xi^j \right) \neq 0. \quad (17)$$

The coefficient of ξ^0 in the left side of (17) is equal to $\hat{w}_0 + h_0 \sum_{s=0}^{n-1-k} \gamma_s b_{m-1,s}$. Under condition (16) in view of $\hat{w}_0 \in W$ we obtain $\hat{w}_0 + h_0 \sum_{s=0}^{n-1-k} \gamma_s b_{m-1,s} \neq 0$, and the validity of condition (17) is established. So, v is a skew MP LRS of order m .

Let us show that v is a non-linearized skew MP LRS. The following condition is fulfilled

$$\dim_R(\tilde{\zeta}(S) \cap S) = k \in \overline{1, n-1}.$$

Therefore, by the second item of Lemma 10 a sequence v is a non-linearized skew MP LRS.

The author is grateful to the Professor A.A. Nechaev for the attention to the work and help in the preparing the manuscript.

References

- [1] *Goltvanitsa M.A., Nechaev A.A., Zaitsev S.N.* Skew linear recurring sequences of maximal period over Galois rings // *Fund. Appl. Math.* — 2011/2012. — V. 17. №3. — P. 5–23. (in Russian).
- [2] *Goltvanitsa M.A., Nechaev A.A., Zaitsev S.N.* Skew LRS of maximal period over Galois rings // *Mat. Vopr. Kriptogr.* — 2013. — V. 4. №2. — P. 59–72.
- [3] *Lidl R., Niederreiter H.* Finite Fields. — Cambridge University Press, 1983.
- [4] *Kurakin V. L., Mikhalev A. V., Nechaev A. A., and Tsypyshev V. N.* Linear and polylinear recurring sequences over abelian groups and modules // *J. Math. Sci.* — 2000. — V. 102. №6. — P. 4598–4626.
- [5] *Glukhov M.M., Elizarov V.P., Nechaev A.A.* Algebra, v. 2. — Moscow : Gelios ARV, 2003. (in Russian).
- [6] *Tsaban B., Vishne U.* Efficient linear feedback shift registers with maximal period // *Finite fields and their Applications.* — 2002. — V. 8. №2. — P. 256–267.
- [7] *Zeng G., Han W., He K.C.* High efficiency feedback shift register: σ -LFSR // *Cryptology ePrint Archive, Report 2007/114.*
- [8] *Zeng, G., He, K.C., Han, W.* A trinomial type of σ -LFSR oriented toward software implementation // *Science in China. Series F-Inform. Sci.* — 2007. — V. 50. №3. — P. 359–372.
- [9] *Zeng, G., He, K.C., Han, W.* Word oriented cascade jump σ -LFSR // *AAECC 2009. Lect. Notes Comput. Sci.* — 2009. — V. 5527. — P. 127–136.
- [10] *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. №2. — P. 123–134.
- [11] *Sudhir R. Ghorpade, Samrith Ram.* Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields // *Finite Fields and their Appl.* — 2011. — V. 17. №5. — P. 461–472.
- [12] *Kurakin V.L.* The Berlecamp-Massey algorithm over finite rings, modules and bimodules // *Discr. math. and appl.* — 1998. — V. 8. — P. 441–473.