Math-Net.Ru

Общероссийский математический портал

М. А. Goltvanitsa, Эквидистантные фильтрующие генераторы на базе скрученных линейных рекуррент максимального периода над полями, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 2, 71–86

DOI: <https://doi.org/10.4213/mvk253>

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: 52.87.193.239

26 апреля 2023 г., 04:37:18

Equidistant filters based on skew ML-sequences over fields**M. A. Goltvanitsa**

Certification Research Center, LLC, Moscow

Получено 05.II.2017

Abstract. 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 recurring sequence v of order m over the module ${}_S S$ is said to be a *skew linear recurring 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 we investigate periodic properties and rank (linear complexity) of the sequence $y(i) = v(i)v(i+k) \cdot \dots \cdot v(i+k(s-1))$, $k, s \in \mathbb{N}_0$, $i \geq 0$, where v is a skew MP LRS. Based on the obtained results we propose new methods for filtering generators construction based on skew MP LRS.

Keywords: linear complexity, period, equidistant filter, skew linear recurrence

Эквидистантные фильтрующие генераторы на базе скрученных линейных рекуррент максимального периода над полями

М. А. Гольтованица

ООО «Центр сертификационных исследований», 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 также $\check{S}$ — кольцо всех линейных преобразований пространства ${}_R S$. Линейную рекуррентную последовательность v порядка m над модулем ${}_S S$ будем называть *скрученной линейной рекуррентной последовательностью (скрученной ЛРП) порядка m над S* . Период $T(v)$ такой последовательности удовлетворяет неравенству $T(v) \leq \tau = q^{mn} - 1$. Если $T(v) = \tau$, то будем называть v *скрученной ЛРП максимального периода (скрученной ЛРП МП)*. В работе исследуются период и ранг последовательности $y(i) = v(i)v(i+k) \cdot \dots \cdot v(i+k(s-1))$, $k, s \in \mathbb{N}_0$, $i \geq 0$, где v — скрученная ЛРП МП. На основе полученных результатов предлагаются новые подходы к построению фильтрующих генераторов с использованием ЛРП МП.

Ключевые слова: ранг последовательности, период, эквидистантный фильтрующий генератор, скрученная линейная рекуррентная последовательность

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 2, pp. 71–86 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

1. Introduction. Preliminaries

Below $R = \mathbb{F}(q)$ is a Galois field with identity e , $q = p^r$, $p = \text{char} R$, $S = \mathbb{F}(q^n)$, $n \geq 2$, is an extension of R with multiplicative group S^* [1]. Let σ be a generator of the group $\text{Aut}(S/R)$ of automorphisms of S over R . Then $\text{ord} \sigma = n$ [1]. 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 defining 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

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

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 recurring sequence (LRS)* of order m over S , if it is a LRS of order m over the module ${}_S S$ [2], 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 $\forall i \in \mathbb{N}_0 \ v(i+m) = \sum_{j=0}^{m-1} \psi_j (v(i+j))$. By $L_S(\Psi)$ we denote the set of all skew LRS over S with a characteristic polynomial Ψ . If $\Psi(x) \in S[x]$, then we call LRS from $L_S(\Psi)$ *classical LRS*.

It is easy to see that a period of any skew LRS v of order m over S satisfies the inequality: $T(v) \leq \tau = q^{nm} - 1$. If $T(v) = \tau$, then we say that v is a skew LRS of *maximal period (MP LRS)* or *maximal length sequence (ML-sequence)*.

Skew MP LRS over Galois rings and finite fields were studied earlier in [2–10]. Systematic research of skew MP LRS over Galois rings was started in [3–5], where, in particular, the results allowing to construct large classes of such sequences without brute force method were developed. In [4, 8–10] the classes of skew MP LRS useful for fast implementation are constructed.

We define the *rank* of the sequence $u \in S^{(1)}$ (and denote it by $\text{rank}_S u$) as the degree of its minimal polynomial over S [1, 19]. In [3] it was shown that the rank of skew MP LRS of order m over S may be n times greater than the rank of classical MP LRS of the same order. Rank and statistical properties are among the most important cryptographic characteristics of pseudorandom sequences [11–13]. Skew MP LRS exhibit good statistical properties, but their ranks are still not high enough. To eliminate this disadvantage we offer in this paper to use the well-known technique based on nonlinear filtering [11–13].

This technique consists in application of non-linear function to the stages of LRS. There is an extensive literature devoted to the derivation of the upper bounds of filtered sequences ranks (see for example [16] and cited literature). However, there are only few fundamentally different constructions for which it is possible to obtain the lower bounds of filtered sequences ranks. The aim of this paper is the study of filtering functions constructions allowing to obtain pseudorandom sequences with guaranteed large rank and period.

Let v be a skew MP LRS of order m over S . Proposed methods for the construction of non-linear filtering functions are based on the results for the sequences of the form

$$y(i) = v(i)v(i+k) \cdot \dots \cdot v(i+k(s-1)), \quad k, s \in \mathbb{N}, \quad 2 \leq s \leq m. \quad (1)$$

Using the terminology from [17] we say that the sequence y is obtained from LRS v by *equidistant filtering*. In the case where v is a classic MP LRS the rank of sequence (1) was investigated in many papers among which we mention [11, 13, 14, 15, 17, 18]. Also it was noted in [15] that sequence (1) has been investigated by V.I. Nechaev, A.A. Nechaev and V.L. Kurakin. Many papers ([13, 14, 17]) were devoted to the case $S = \mathbb{F}(2)$ or to the case $S = \mathbb{F}(2^n)$ [18]. In papers [11] and [15] the sequence (1) was investigated over the arbitrary finite field, for the cases $s = 2$ and $k = 1$, respectively. In all mentioned papers, except [11] it was supposed that the sequence (1) satisfies the condition $(k, \tau) = 1$, where (k, τ) is the greatest common divisor of k and τ .

In the present paper we study the case where v is a skew MP LRS. We extend the class of sequences studied by removing the restriction $(k, \tau) = 1$. Along with the case of field of characteristic 2 we investigate the general case. Also we investigate the periodic properties of sequence (1).

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

Theorem 1 ([3]). *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 a primitive polynomial $F(x) \in R[x]$ of degree mn such that $v \in L_S(F)$.*

Let conditions of Theorem 1 are satisfied and α be a root of the polynomial $F(x)$ in the extension $K = \mathbb{F}(q^{mn})$ of the field S [1]. Then $F(x)$ has a canonical decomposition over S :

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

where $F_0(x), \dots, F_{n-1}(x)$ are primitive polynomials of degree m over S [1]. Therefore, every $v \in L_S(F)$ has a unique decomposition $v = w_0 + \dots + w_{n-1}$, where $w_j \in L_S(F_j)$ [19].

Let tr_S^K be a trace-function from the field K onto the field S [1]. Then for every $j \in 0, n-1$ there exists a unique element $\varepsilon_j \in K$ such that $w_j(i) = \text{tr}_S^K(\varepsilon_{jj}^i)$, $i \geq 0$ [19]. So we obtain the following decomposition for the LRS v :

$$v(i) = \text{tr}_S^K(i)_0 + \text{tr}_S^K(iq)_1 + \cdots + \text{tr}_S^K(iq^{n-1})_{n-1}. \quad (2)$$

The tuple $(\varepsilon_0, \dots, \varepsilon_{n-1})$ is called *the defining tuple of factors* of LRS v . The approach to the description and construction of skew MP LRS based on defining tuples of factors was proposed in [5].

Further in this paper v is a skew MP LRS with the defining tuple of factors $(0, \dots, n-1)$, i.e. condition (2) is fulfilled.

We put $N(v) = \{j \in 0, n-1 : \varepsilon_j \neq 0\}$, $|N(v)| = n_0$. The rank of sequence (2) is equal to mn_0 and in the case where $n_0 = 1$ the sequence v is a classical MP LRS from the set $L_S(F)$. The methods of construction of skew MP LRS over S having order m and the highest rank mn were described in papers [5, 8].

For any element $\in K$ denote by $[R():R]$ the degree of the field extension $R()$ over the field R [19]. For every integer $\nu \in 1, m$ such that $\nu|m$ we introduce the notation

$$D_s(m, n_0, \nu) = n_0^s \binom{\nu}{s} \left(\frac{m}{\nu}\right)^s + (n_0)_s \left(\binom{m}{s} - \binom{\nu}{s} \left(\frac{m}{\nu}\right)^s \right) + \binom{n_0}{s} m, \quad (3)$$

where $(n_0)_s = n_0(n_0-1) \cdots (n_0-s+1)$ if $n_0 \geq s$ and $(n_0)_s = 0$ if $n_0 < s$. We recall that y is a sequence of the form (1).

Theorem 2. *Let*

$$[R^{(k)}:R] = \mu, \quad n|\mu, \quad \nu = \frac{\mu}{n}. \quad (4)$$

1. *If $\text{char } R \neq 2$, $s = 2$, and k satisfies the condition*

$$[R^{(2k)}:R] = [R^{(k)}:R], \quad (5)$$

then

$${}_S y = \frac{mn_0(mn_0+1)}{2}. \quad (6)$$

2. *In the case $\text{char } R = 2$ we have*

$${}_S y \geq D_s(m, n_0, \nu), \quad (7)$$

and if $s < q$, then

$${}_S y \geq D_s(m, n_0, \nu) + mn_0. \quad (8)$$

3. *In the case $\text{char } R = 2$ and $s = 2$ the following equality is fulfilled:*

$${}_S y = D_2(m, n_0, \nu) + mn_0. \quad (9)$$

As was noted above, in the previous papers on the classical LRS mainly the case $(k, \tau) = 1$ was investigated. In this case $\mu = mn$, $\nu = m$ and from (3) we obtain

$$D_s(m, n_0, \nu) = n_0^s \binom{m}{s} + \binom{n_0}{s} m. \quad (10)$$

For classic MP LRS we have $n_0 = 1$, so it follows from (10) and Theorem 2 that the lower bound for ${}_s y$ may be n^s times larger than the corresponding lower bound for ${}_s y$ in the case of a classical MP LRS v . Thus, the best lower bounds for ${}_s y$ we obtain in the case of skew MP LRS v such that ${}_s v = mn$.

Theorem 3. *The period $T(y)$ of the sequence y satisfies the condition*

$$T(y) \mid \frac{\tau}{(q-1, s)}. \quad (11)$$

If $s = 2$, then

$$T(y) = \frac{\tau}{(q-1, 2)}. \quad (12)$$

If $\text{char } R = 2$ and condition (4) is fulfilled, then

1) for $m < s$

$$\frac{\tau}{(q^n - 1, s)} \mid T(y), \quad (13)$$

2) for $3 \leq s < m$ and $n_0 \geq 2$

$$\frac{\tau}{(q^\lambda - 1, s)} \mid T(y), \quad (14)$$

where λ is the greatest common divisor of all elements from the set

$$\{j_b - j_a : j_a, j_b \in N(v), a, b \in 1, n_0, j_a < j_b\} \cup \{n\}.$$

Corollary. *Let conditions of Theorem 2 be satisfied along with conditions $\text{char } R = 2$, $3 \leq s < m$. Then if any of two conditions*

1) $n_0 \geq 2$ and n is prime,

2) $n_0 > n/2$,

is fulfilled, then the period of sequence y takes the maximal possible value:

$$T(y) = \frac{\tau}{(q-1, s)}. \quad (15)$$

The validity of Corollary follows from the fact that if the conditions of the first or the second item are fulfilled then the value of λ in Theorem 3 is equal to 1.

From the Corollary it follows that skew MP LRS v with $sv = mn$ is preferable to obtain the maximum value of $T(y)$.

Obtained results permit us to propose one class of functions for filtering generator construction based on skew MP LRS. Recall (see for example [1]) that for every function $f: S^m \rightarrow S$ there exists a unique representation of the form

$$f(x_1, x_2, \dots, x_m) = \sum_{\mathbf{l} \in 0, q^n - 1^m} a_{l_1 l_2 \dots l_m} x_1^{l_1} x_2^{l_2} \dots x_m^{l_m},$$

where $\mathbf{l} = (l_1, l_2, \dots, l_m)$, $l_j \in 0, q^n - 1$, $j \in 1, m$, $a_{l_1 \dots l_m} \in S$, and a *degree* $\deg f$ of f is defined as $\max\{l_1 + l_2 + \dots + l_m : a_{l_1 l_2 \dots l_m} \neq 0\}$. The degree of zero function is equal to zero.

Let $f: S^m \rightarrow S$ be a function such that $\deg f < s$. Consider the sequence

$$z(i) = \sum_{j=0}^{N-1} h_j y(i+j) + f(v(i), v(i+1), \dots, v(i+m-1)), \quad (16)$$

where $h_0, h_1, \dots, h_{N-1}$ are arbitrary elements from S such that not all of them are equal to zero and y is sequence (1).

Theorem 4. *Let conditions of Theorem 2 are fulfilled. If $\text{char } R = 2$, then*

$$sz \geq D_s(m, n_0, \nu) - (N - 1). \quad (17)$$

If $\text{char } R \neq 2, s = 2$ and k satisfies (5), then

$$sz \geq D_2(m, n_0, m) - (N - 1). \quad (18)$$

The author is grateful to Professor A. A. Nechaev and Professor A. S. Kuzmin for helpful discussions and valuable remarks.

2. Proofs

Below we use the notation $\mathbf{j} = (j_1, \dots, j_s)$, $\mathbf{l} = (l_1, \dots, l_s)$. We put $J = N(v)^s$ and decompose the sequence y into the sum of binomial sequences [19]:

$$\begin{aligned} y(i) &= v(i)v(i+k) \cdot \dots \cdot v(i+k(s-1)) = \\ &= \left(\sum_{l=0}^{m-1} \sum_{j \in N(v)} \binom{q^{nl}}{j} i q^{nl+j} \right) \cdot \dots \cdot \left(\sum_{l=0}^{m-1} \sum_{j \in N(v)} \binom{q^{nl}}{j} k^{(s-1)} q^{nl+j} i q^{nl+j} \right) = \\ &= \sum_{(j_1, \dots, j_s) \in J} \sum_{0 \leq l_1, \dots, l_s \leq m-1} \left(\prod_{a=1, s}^{q^{nl_a}} \binom{k(a-1)q^{nl_a+j_a}}{j_a} \right) i^{\sum_{a \in 1, s} q^{nl_a+j_a}}. \end{aligned}$$

So, the i th term $y(i)$ of LRS y has the representation

$$y(i) = \sum_{0 \leq l_1, \dots, l_s \leq m-1, \mathbf{j} \in J, n l_a + j_a \leq n l_b + j_b, a, b \in 1, s, a < b} c_{\mathbf{j}1} (q^{n l_1 + j_1 + \dots + q^{n l_s + j_s}})^i, \quad c_{\mathbf{j}1} \in K. \quad (19)$$

We define two sets

$$W = \{(l_1, \dots, l_s), l_a \in 0, m-1, a \in 1, s, l_a \neq l_b, a \neq b, a, b \in 1, s\},$$

$$W_1 = \begin{cases} \{(j_1, \dots, j_s) \in J, j_a \neq j_b, a \neq b, a, b \in 1, s\}, & s \leq n_0, \\ \emptyset, & s > n_0. \end{cases}$$

Then $y(i) = y'(i) + \tilde{y}(i) + y''(i)$, where

$$y'(i) = \sum_{\mathbf{j} \in J} \sum_{\mathbf{l} \in W} \left(\prod_{a \in 1, s}^{q^{n l_a}} j_a \right) \cdot k q^{n l_2 + j_2} \dots k^{(s-1)} q^{n l_s + j_s} i^{\sum_{a \in 1, s} q^{n l_a + j_a}}, \quad (20)$$

$$\tilde{y}(i) = \begin{cases} \sum_{\mathbf{j} \in W_1} \sum_{l=0}^{m-1} \left(\prod_{a \in 1, s}^{q^{n l}} j_a \right) \cdot k q^{n l + j_2} \dots k^{(s-1)} q^{n l + j_s} i^{\sum_{a \in 1, s} q^{n l + j_a}}, & s \leq n_0, \\ 0, & s > n_0, \end{cases} \quad (21)$$

$$y''(i) = y(i) - y'(i) - \tilde{y}(i).$$

Lemma 5. *Minimal polynomials of the sequences y' , $\tilde{y}$ and y'' over K are coprime.*

Proof. Consider the case $s \leq n_0$. The sequences y' , $\tilde{y}$ and y'' are binomial sequences of the first order. So to prove Lemma 5 it is sufficient to show that the sets of roots of binomial sequences from the corresponding decompositions are disjoint.

Since $n \geq 2$, $s \leq m$, we obtain that for every $\mathbf{j} \in J$, $\mathbf{l} \in W$ the following inequalities are valid

$$\sum_{t=1}^s q^{n l_t + j_t} \leq q^{n-1} \sum_{t=0}^{m-1} q^{n t} = q^{n-1} \frac{q^{mn} - 1}{q^n - 1} < q^{mn} - 1 = \text{ord}.$$

Further, for all $\mathbf{j} \in W_1$, $l \in 0, m-1$,

$$\sum_{t=1}^s q^{n l + j_t} \leq q^{n(m-1)} \sum_{t=0}^{n-1} q^t = q^{n(m-1)} \frac{q^n - 1}{q - 1} < q^{mn} - 1 = \text{ord}.$$

So, the set of roots of binomial sequences from the y' decomposition (20) is disjoint with the corresponding set from the $\tilde{y}$ decomposition (21).

Now we show that if $s = 2$ or $\text{char } R = 2$, then the set of roots of binomial sequences from the y' decomposition is disjoint with the analogous set of roots of binomial sequences roots from the y'' decomposition. For $s = 2, q > 2$ this follows from the fact that all roots of binomial sequences in the decomposition (19) are pairwise distinct since

$$\sum_{a=1}^s q^{nl_s+j_s} \leq sq^{(m-1)n+n-1} = sq^{mn-1} < q^{mn} - 1 = \text{ord}. \quad (22)$$

Further we consider the case $\text{char } R = 2$. Assume the contrary: let there exist the tuples

$$(l_1, \dots, l_s, j_1, \dots, j_s), (\tilde{l}_1, \dots, \tilde{l}_s, \tilde{j}_1, \dots, \tilde{j}_s), \quad l_t, \tilde{l}_t \in 0, m-1, \quad j_t, \tilde{j}_t \in N(v),$$

such that $l_a \neq l_b$ if $a \neq b, a, b \in 1, s$, and

$$q^{nl_1+j_1} + \dots + q^{nl_s+j_s} \equiv q^{n\tilde{l}_1+\tilde{j}_1} + \dots + q^{n\tilde{l}_s+\tilde{j}_s} \pmod{q^{mn} - 1}. \quad (23)$$

Since $\text{char } S = 2$, the congruence (23) has the form

$$2^{t_1} + \dots + 2^{t_s} \equiv 2^{\tilde{t}_1} + \dots + 2^{\tilde{t}_s} \pmod{2^h - 1}, \quad (24)$$

where $2^{t_i} = q^{nl_i+j_i}$, $2^{\tilde{t}_i} = q^{n\tilde{l}_i+\tilde{j}_i}$ for all $i \in 1, s$, $h = mn \log_2 q$, and $t_i \neq t_j$ if $i \neq j, i, j \in 1, s$. If $\tilde{t}_i \neq \tilde{t}_j$ for all $i, j \in 1, s, i \neq j$, then the congruence (24) is equivalent to the equality

$$2^{t_1} + \dots + 2^{t_s} = 2^{\tilde{t}_1} + \dots + 2^{\tilde{t}_s},$$

which is impossible because of the condition $(t_1, \dots, t_s) \neq (\tilde{t}_1, \dots, \tilde{t}_s)$.

If there exist $i, j \in 1, s, i \neq j$, such that $\tilde{t}_i = \tilde{t}_j$, then grouping equal terms in the right side of the congruence (24) and replacing, if necessary, 2^h by 1, we obtain the equality

$$2^{t_1} + \dots + 2^{t_s} = 2^{\hat{t}_1} + \dots + 2^{\hat{t}_w},$$

where $w < s$ and $\hat{t}_i \neq \hat{t}_j$ under $i \neq j$. This is a contradiction. Similarly it may be established that minimal polynomials of sequences $\tilde{y}$ and y'' are coprime.

If $s > n_0$, then $\tilde{y}$ is zero-sequence and its minimal polynomial is equal to e . So, in this case it is sufficient to prove that minimal polynomials of sequences y' and y'' are coprime, but this what has been done above. Lemma 5 is proved. $\square$

2.1. Proof of Theorem 2

First we prove item 2. We note that $y', \tilde{y}$ are the sequences over K . So, from condition $S \subset K$ we obtain:

$${}_K y' \leq_S y', \quad {}_K \tilde{y} \leq_S \tilde{y}. \quad (25)$$

In the following two lemmas we estimate the ranks of the sequences y' and $\tilde{y}$ as LRS over K , and then use the corresponding inequality from (25).

Lemma 6. *The rank of the sequence y' satisfies the inequality*

$${}_K y' \geq n_0^s \binom{\nu}{s} \left(\frac{m}{\nu}\right)^s + (n_0)_s \left(\binom{m}{s} - \binom{\nu}{s} \left(\frac{m}{\nu}\right)^s \right). \quad (26)$$

Proof. Let

$$L = \{(l_1, \dots, l_s) : 0 \leq l_1 < \dots < l_s \leq m-1\}.$$

Using (20) we obtain the decomposition

$$y'(i) = \sum_{\mathbf{j} \in J} \sum_{\mathbf{l} \in L} c'_{\mathbf{j}\mathbf{l}} (q^{nl_1+j_1} + \dots + q^{nl_s+j_s})^i, \quad c'_{\mathbf{j}\mathbf{l}} \in K. \quad (27)$$

Let $\mathcal{P}(1, s)$ be the set of all permutations of the set $1, s$ [19]. Sequence (27) is the sum of binomial sequences of the first order with distinct roots, wherein using (20) we get that the coefficient $c'_{\mathbf{j}\mathbf{l}}$ is equal to

$$c'_{\mathbf{j}\mathbf{l}} = \sum_{(\rho_1, \dots, \rho_s) \in \mathcal{P}(1, s)}^{q^{nl_{\rho_1}}} j_{\rho_1} \dots j_{\rho_s}^{q^{nl_{\rho_s}}} k q^{nl_{\rho_2}+j_{\rho_2}+\dots+k(s-1)q^{nl_{\rho_s}+j_{\rho_s}}}. \quad (28)$$

Since $\text{char } R = 2$, then using (28) we obtain

$$c'_{\mathbf{j}\mathbf{l}} = \begin{vmatrix} q^{nl_1} & q^{nl_2} & \dots & q^{nl_s} \\ j_1 & j_2 & \dots & j_s \\ q^{nl_1} k q^{nl_1+j_1} & q^{nl_2} k q^{nl_2+j_2} & \dots & q^{nl_s} k q^{nl_s+j_s} \\ \dots & \dots & \dots & \dots \\ q^{nl_1} k(s-1)q^{nl_1+j_1} & q^{nl_2} k(s-1)q^{nl_2+j_2} & \dots & q^{nl_s} k(s-1)q^{nl_s+j_s} \end{vmatrix}. \quad (29)$$

For any elements $\xi_1, \dots, \xi_t \in K$ denote by $V(\xi_1, \dots, \xi_t)$ the Vandermonde determinant, that is $V(\xi_1, \dots, \xi_t) = \det(\xi_j^{i-1})_{i,j=1}^t$.

Recall (see, for example, [19]) that condition $V(\xi_1, \dots, \xi_t) \neq 0$ is equivalent to the condition $\xi_a \neq \xi_b$, $a, b \in 1, t$, $a \neq b$.

Using (29) we have $c'_{\mathbf{j}\mathbf{l}} = \prod_{j_1=1}^{q^{n_{l_1}}} \dots \prod_{j_s=1}^{q^{n_{l_s}}} V(kq^{n_{l_1}+j_1}, \dots, kq^{n_{l_s}+j_s})$.

So, coefficient (28) is not zero iff

$$kq^{n_{l_a}+j_a} \neq kq^{n_{l_b}+j_b}, \quad a, b \in 1, s, \quad a \neq b. \quad (30)$$

We consider two cases. First, if all coordinates of the vector $\mathbf{j}$ are pairwise distinct, then the condition (30) is fulfilled for all $\mathbf{l} \in L$. Indeed, condition (30) is valid iff

$$\mu \nmid n(l_a - l_b) + (j_a - j_b), \quad a, b \in 1, s, \quad a \neq b. \quad (31)$$

Using equality $\mu = n\nu$, we find that the last condition is true since $n \nmid j_a - j_b$. So, in this case there are exactly

$$(n_0)_s \binom{m}{s} \quad (32)$$

non-zero coefficients $c'_{\mathbf{j}\mathbf{l}}$ of the form (28).

Second, if there exist $a, b \in 1, s$ such that $a \neq b$ and $j_a = j_b$, then arguing similarly and taking into account (31) and equality $\mu = n\nu$ we obtain that the validity of condition (30) follows from the condition $\mu \nmid n(l_a - l_b)$, $a, b \in 1, s$, i. e. l_a and l_b are not congruent modulo ν . There exist exactly $n_0^s - (n_0)_s$ tuples $\mathbf{j} \in J$ with at least two equal coordinates and there is exactly

$$\binom{\nu}{s} \left(\frac{m}{\nu}\right)^s$$

tuples $\mathbf{l} \in L$ with coordinates pairwise non-congruent modulo ν . So, in the case where there exists at least one pair of equal coordinates of $\mathbf{j} \in J$ there are at least

$$(n_0^s - (n_0)_s) \binom{\nu}{s} \left(\frac{m}{\nu}\right)^s \quad (33)$$

non-zero coefficients $c'_{\mathbf{j}\mathbf{l}}$ of the form (28).

So, Ky' is not smaller than the sum of values (33) and (32). Lemma 6 is proved.

□

Lemma 7. *The following equality is true:*

$${}_K\tilde{y} = \binom{n_0}{s} m. \quad (34)$$

Proof. We note that if $s > n_0$, then $\tilde{y}$ is the zero sequence and the equality (34) is fulfilled. Consider the case $s \leq n_0$. Using (21) we find that the sequence $\tilde{y}$ has the form

$$\tilde{y}(i) = \sum_{(j_1, \dots, j_s) \in J, j_1 < \dots < j_s} \sum_{l=0}^{m-1} \tilde{c}_{lj}^{(q^{nl+j_1} + \dots + q^{nl+j_s})i}, \quad (35)$$

where the $\tilde{c}_{lj}$ may be calculated by the formula

$$\tilde{c}_{lj} = \left(\sum_{(\rho_1, \dots, \rho_s) \in \mathcal{P}(1, s)} j_{\rho_1} \cdot \dots \cdot j_{\rho_s}^{kq^{j\rho_2} + \dots + k(s-1)q^{j\rho_s}} \right)^{q^{nl}}. \quad (36)$$

Further, since $\text{char} S = 2$ we obtain that coefficient (36) is not equal to zero iff the element $j_1 \cdot \dots \cdot j_s V(kq^{j_1}, \dots, kq^{j_s})$ is not equal to zero. The last condition is equivalent to the pairwise non-congruence modulo μ of numbers $j_a, j_b \in N(v)$, where $a \neq b$, $a, b \in 1, s$. Since $n \mid \mu$, we have $\mu \geq n$ and $\mu \nmid j_a - j_b \in \{-n+1, -n+2, \dots, n-1\}$. So, ${}_K\tilde{y}$ is equal to the number of non-zero coefficients (36), that is to the number $\binom{n_0}{s} m$. Lemma 7 is proved. $\square$

Now the validity of (7) follows from Lemmas 5–7.

Let us show that if $s < q$, then the inequality (8) is valid. Since $s < q$ we find that all roots of binomial sequences if (19) are pairwise distinct (see (22)). Further, the coefficient c_{jl} in decomposition (19) with

$$\mathbf{l} = (l, l, \dots, l), \quad \mathbf{j} = (j, j, \dots, j) \quad (37)$$

for every $l \in 0, m-1$, $j \in N(v)$, is equal to

$$c_{lj} = \binom{s}{j} q^{nl} \binom{s}{2} k q^{nl+j} \neq 0.$$

There are exactly mn_0 pairs of vectors (37). Now the validity of (8) follows from the validity of (7).

Now we prove item of Theorem 2. We need the following result.

Lemma 8. *Let u be LRS over S and ${}_K u = N$. Then ${}_S u = N$.*

Proof. If u is zero sequence, then its minimal polynomials over S and over K coincides and are equal to e . Let $u \neq 0$ and

$$f(x) = x^N - \sum_{j=0}^{N-1} f_j x^j \in K[x]$$

be a minimal polynomial of u , where $N \geq 1$. Then

$$u(i+N) = \sum_{j=0}^{N-1} f_j u(i+j) \quad \text{for every } i \in \mathbb{Z}.$$

Using the equality $|S| = q^n$ from the last condition we obtain [1]

$$u(i+N) = \sum_{j=0}^{N-1} f_j^{q^n} u(i+j).$$

If $f(x) \in S[x]$, then Lemma 8 is valid. Assume that $f(x) \notin S[x]$. Choose the maximal value $j \in \mathbb{Z}$ such that $f_j \notin S$. Then $f_j^{q^n} \neq f_j$ and

$$\left(x^j + (f_j^{q^n} - f_j)^{-1} (f_{j-1}^{q^n} - f_{j-1}) x^{j-1} + \dots + (f_0^{q^n} - f_0)^{-1} (f_0^{q^n} - f_0) \right) \cdot u = 0$$

if $j \geq 1$, or $e \cdot u = 0$, if $j = 0$. So, the sequence u may be annihilated by a monic polynomial of degree $j < N$ over K . This is a contradiction. Thus, $f(x) \in S[x]$. Lemma is proved. $\square$

We note that under the condition $s = 2$ regardless of field characteristic the equality

$${}_K y'' = mn_0$$

is fulfilled. To complete the proof we use Lemmas 5–8. Item 1 of Theorem 2 is proved.

Now we prove item 1 of Theorem 2.

Lemma 9. *If condition (5) is fulfilled, then*

$${}_K y' = n_0^2 \binom{m}{2}. \quad (38)$$

Proof. Since $s = 2$ the coefficient (28) from the decomposition (27) is not equal to zero iff

$$kq^{nl_1+j_1} \neq -kq^{nl_2+j_2}.$$

We put

$$\begin{aligned} C_1 &= \{(\mathbf{j}, \mathbf{l}) \in J \times L : kq^{nl_1+j_1} \neq -kq^{nl_2+j_2}\}, \\ C_2 &= \{(\mathbf{j}, \mathbf{l}) \in J \times L : kq^{nl_1+j_1} \neq kq^{nl_2+j_2}\}, \\ C_3 &= \{(\mathbf{j}, \mathbf{l}) \in J \times L : 2kq^{nl_1+j_1} \neq 2kq^{nl_2+j_2}\}. \end{aligned}$$

So, ${}_K y' = |C_1|$. We obtain

$$|C_1| = (|J| \cdot |L| - |C_2|) + |C_3|,$$

since $\text{char } R \neq 2$. Using (5) we get $|C_2| = |C_3|$. So,

$${}_K y' = |C_1| = |J| \cdot |L| = n_0^2 \binom{m}{2}.$$

Lemma is proved. □

Arguing analogously to the proof of Lemma 9, we get

$${}_K \tilde{y} = \binom{n_0}{2} m. \quad (39)$$

As it was noted above, ${}_K y'' = mn_0$. Now using Lemma 8 we get

$${}_S y = n_0^2 \binom{m}{2} + m \binom{n_0}{2} + mn_0 = \binom{mn_0 + 1}{2}.$$

2.2. Proof of Theorem 3

We show that

$$T(y) \mid \frac{q^{mn} - 1}{(q - 1, s)}.$$

Let

$$\Delta = \frac{q^{mn} - 1}{q - 1},$$

then

$$v(i + \Delta) = \text{tr}_S^K \left(\sum_{j=0}^{n-1} q^j (i + \Delta) \right) = \text{tr}_S^K \left(\sum_{j=0}^{n-1} \Delta q^j q^j i \right). \quad (40)$$

Since $\Delta \in R$ from (40) we find

$$v(i + \Delta) = \text{tr}_S^K \left(\sum_{j=0}^{n-1} \Delta q^j q^{ji} \right) =^\Delta v(i). \quad (41)$$

Using (1) and (41) we get $y(i + \Delta) =^{s\Delta} y(i)$. So,

$$T(y) | \Delta \cdot \text{ord}^{s\Delta} = \frac{\tau}{q-1} \cdot \frac{q-1}{(q-1, s)} = \frac{\tau}{(q-1, s)}.$$

Now we prove (12). Since the minimal polynomials of the sequences y' , $\tilde{y}$ and y'' are pairwise coprime, the relation $T(y'')|T(y)$ is valid [19]. As it was noted above, in the case $s = 2$ the sequence y'' is the sum of binomial sequences with the roots from the set

$$M(y'') = \{q^{2q^{nl+j}}, l \in 0, m-1, j \in N(v)\}.$$

So, the period $T(y'')$ of LRS y'' is equal to the least common multiple (LCM) of orders of elements from $M(y'')$, that is to the number $\tau/(\tau, 2)$. Now (12) follows from the equality

$$\frac{\tau}{(\tau, 2)} = \frac{\tau}{(q-1, 2)}.$$

Now we prove (13). Since the minimal polynomials of the sequences y' , $\tilde{y}$ и y'' are pairwise coprime, the relation $T(y')|T(y)$ is valid [19]. Using (27) we find that the period $T(y')$ of the sequence y' is equal to the LCM of orders of elements from the set

$$M(y') = \{q^{n l_1 + j_1 + \dots + q^{n l_s + j_s}}, \mathbf{j} \in J, \mathbf{l} \in L, c'_{j_1} \neq 0\}.$$

For $j_1 \in N(v)$ we define the numbers

$$= q^{j_1} + q^{2n+j_1} + \dots + q^{ns+j_1}, \quad \beta = q^{n+j_1} + q^{2n+j_1} + \dots + q^{ns+j_1}.$$

From the proof of Lemma 6 it follows that $\beta \in M(y')$. It is easy to see that $[\text{ord}, \text{ord}^\beta] = \tau/(\tau, \beta)$, where by $[k_1, \dots, k_l]$ we denote the LCM of the numbers $k_1, \dots, k_l$. Now to prove (13) it is sufficient to note that

$$(\tau, \beta) = (\tau, \beta, \beta-) = (\tau, \beta, q^{j_1}(q^n - 1)) = (q^n - 1, s). \quad (42)$$

Now we establish (14). For every $j_a, j_b \in N(v)$ such that $j_a < j_b$ we define the numbers

$$\begin{aligned} \gamma_{ab} &= q^{j_a} + q^{n+j_b} + q^{2n+j_a} + \dots + q^{n(s-1)+j_a}, \\ \tilde{\gamma}_{ab} &= q^{j_b} + q^{n+j_b} + q^{2n+j_a} + \dots + q^{n(s-1)+j_a}. \end{aligned}$$

From the proof of Lemma 6 it follows that $\gamma_{ab}, \tilde{\gamma}_{ab} \in M(y')$. It is easy to see that for any fixed $j_a, j_b \in N(v)$, $a \neq b$, we have

$$[\text{ord}, \text{ord}^\beta, \text{ord}^{\gamma_{ab}}, \text{ord}^{\tilde{\gamma}_{ab}}] = \frac{q^{mn} - 1}{(q^{mn} - 1, \beta, \gamma_{ab}, \tilde{\gamma}_{ab})}.$$

Further, $(q^{mn} - 1, \beta, \gamma_{ab}, \tilde{\gamma}_{ab}) = ((q^{mn} - 1, \beta), \gamma_{ab}, \tilde{\gamma}_{ab})$. Thus, using (42) we find that the value $(q^{mn} - 1, \beta, \gamma_{ab}, \tilde{\gamma}_{ab})$ divides

$$(q^n - 1, s, \tilde{\gamma}_{ab} - \gamma_{ab}) = (q^n - 1, s, q^{j_b} - q^{j_a}) = (q^{(n, j_b - j_a)} - 1, s).$$

Looking over all elements $j_a, j_b \in N(v)$, $j_a < j_b$ and arguing similarly we establish (14). Theorem 3 is completely proved.

2.3. Proof of Theorem 4

Let $H(x) = \sum_{j=0}^{N-1} h_j x^j$. Then $z(i) = z'(i) + \tilde{z}(i) + z''(i) + \hat{z}(i)$, where

$$\begin{aligned} z'(i) &= H(x)y'(i), \quad \tilde{z}(i) = H(x)\tilde{y}(i), \quad z''(i) = H(x)y''(i), \\ \hat{z}(i) &= z(i) - z'(i) - \tilde{z}(i) - z''(i). \end{aligned} \quad (43)$$

For every number $k = \sum_{t \geq 0} \nu_s(k) q^k \in \mathbb{F}_q$, $\nu_s(k) \in \mathbb{F}_q$, we define its weight $\text{wt}_q(k)$ as the arithmetic sum $\text{wt}_q(k) = \sum_{t \geq 0} \nu_t(k)$. Using (2) and condition $\deg f < s$ we find that the sequence $\hat{z}(i)$ is the sum of binomial sequences of the first order with the roots β , where $\beta < \tau$, $\text{wt}_q \beta < s$. As was shown above all roots β , where $\beta < \tau$ of non-zero binomial sequences from the decomposition of y' satisfy the equality $\text{wt}_q \beta = s$, and therefore all roots from binomial decomposition of z' satisfy the same equality. For every sequence u over K denote by $m_u(x)$ its minimal polynomial over K . So, we establish the equalities $(m_{z'}(x), m_{\hat{z}}(x)) = e$ and $(m_{\tilde{z}}(x), m_{\hat{z}}(x)) = e$ (we use the notation $(G(x), L(x))$ for the greatest common divisor of polynomials $G(x), L(x) \in K[x]$).

Taking into account Lemma 5 we obtain $(m_{z'+\tilde{z}}(x), m_{z''+\hat{z}}(x)) = e$ and therefore $s z \geq_K z \geq_K (z' + \tilde{z})$. Using (43) we get [19]

$$K(z' + \tilde{z}) = \deg m_{z'+\tilde{z}}(x) = \deg \frac{m_{y'+\tilde{y}}(x)}{(m_{y'+\tilde{y}}(x), H(x))}.$$

In the case $\text{char } R = 2$ by means of Lemmas 5–7 we find that

$$\begin{aligned} \deg \frac{m_{y'+\tilde{y}}(x)}{(m_{y'+\tilde{y}}(x), H(x))} &\geq \deg m'_y + \deg m_{\tilde{y}}(x) - \deg H(x) \\ &\geq D_s(m, n_0, \nu) - (N - 1). \end{aligned}$$

If $\text{char } R \neq 2$, $s = 2$ and k satisfies (5), then using (38) and (39) we obtain (18). Theorem 4 is proved. $\square$

References

- [1] Lidl R., Niederreiter H., *Finite Fields*: Cambridge Univ. Press, 1983, 755 pp.
- [2] 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.*, **102**:6 (2000), 4598–4626.
- [3] Goltvanitsa M.A., Nechaev A.A., Zaitsev S.N., “Skew linear recurring sequences of maximal period over Galois rings”, *J. Math. Sci.*, **187**:2 (2012), 115–128.
- [4] Goltvanitsa M.A., Nechaev A.A., Zaitsev S.N., “Skew LRS of maximal period over Galois rings”, *Matem. Voprosy Kriptografii*, **4**:2 (2013), 59–72.
- [5] Goltvanitsa M.A., “A construction of skew LRS of maximal period over finite fields based on the defining tuples of factors”, *Matem. Voprosy Kriptografii*, **5**:2 (2014), 37–46.
- [6] Goltvanitsa M.A., “Digit sequences of skew linear recurrences of maximal period over Galois rings”, *Matem. Voprosy Kriptografii*, **6**:2 (2015), 189–197.
- [7] Goltvanitsa M.A., “The first digit sequence of skew linear recurrence of maximal period over Galois ring”, *Matem. Voprosy Kriptografii*, **7**:3 (2016), 5–18.
- [8] Goltvanitsa M.A., “On a class of skew linear recurrences of maximal period over Galois rings”, *Sistemy vysokoi dostupnosti*, **11**:3 (2015), 28–49 (in Russian).
- [9] Tsaban B., Vishne U., “Efficient linear feedback shift registers with maximal period”, *Finite Fields and Their Appl.*, **8**:2 (2002), 256–267.
- [10] Zeng, G., He, K.C., Han, W., “A trinomial type of σ -LFSR oriented toward software implementation”, *Sci. in China, Ser. F – Inf. Sci.*, **50**:3 (2007), 359–372.
- [11] Alferov A.P., Zubov A.U., Kuzmin A.S., Cheremushkin A.V., *Foundations of Cryptography*: Gelios ARV, 2002, 480 pp. (in Russian).
- [12] Menezes A.J., Vanstone S.A., Van Oorschot P.C., *Handbook of Applied Cryptography*: CRC Press, 1996, 780 pp.
- [13] Rueppel R.A., *Analysis and Design of Stream Ciphers*, Heidelberg etc.: Springer-Verlag, 1986, xii+244 pp.
- [14] Bernasconi C., Gunter G., “Analysis of a nonlinear feedforward logic for binary sequence generators”, *Lect. Notes Comput. Sci.*, **219** (1986), 161–166.
- [15] Bogonotov R.V., “Nechaev’s hypothesis on linear recurrences multiplication”, *Chebyshevskii sbornik*, **6**:1, 48–55 (in Russian).
- [16] Kurakin V.L., “Polynomial transformations of linear recurrent sequences over the ring p^2 ”, *Discrete Mathem. and Appl.*, **9**:2 (1999), 185–210.
- [17] Kolokotronis N., Liminotis K., Kaloupsidis N., “Lower bounds on sequence complexity via generalised Vandermonde determinants”, *Lect. Notes Comput. Sci.*, **4086** (2006), 271–284.
- [18] Lam C., Gong G., “A lower bound for the linear span of filtering sequences”. In: “*State of Art of Stream Ciphers (SASC)*”, 2004, 220–233.
- [19] Glukhov M.M., Elizarov V.P., Nechaev A.A., *Algebra*, v.1, 2: Gelios ARV, 2003, 336+415 pp. (in Russian).