M. A. Goltvanitsa, Digit sequences of skew linear recurrences of maximal period over Galois rings,
*Mat. Vopr. Kriptogr.*, 2015, Volume 6, Issue 2, 19–27

**МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ**
**2015 Т. 6 № 2 С. 19–27**

УДК: 519.624+519.113.6

# Digit sequences of skew linear recurrences of maximal period over Galois rings

**M. A. Goltvanitsa**

LLC “Certification Research Center”, Moscow

*Получено 16.IX.2014*

A pseudo-random sequences constructed as a digit sequence of a skew linear recurrence of maximal period over Galois ring are studied. We find the periods of such sequences and lower bounds for their ranks as a sequences over field. A rank of the first digit sequence of a skew linear recurrence of maximal period is determined exactly under certain conditions on the digit set.

Key words: skew linear recurrences, Galois ring, digit sequence

**Разрядные последовательности скрученных линейных рекуррент максимального периода над кольцами Галуа**

**М. А. Гольтваница**

*ООО «Центр сертификационных исследований», г. Москва*

**Аннотация.** Изучаются свойства псевдослучайной последовательности, полученной из разрядной последовательности скрученной линейной рекурренты максимального периода над кольцом Галуа. Для такой последовательности найдены период и нижние оценки ее ранга как последовательности над полем. Для ранга первой разрядной последовательности скрученной линейной рекурренты максимального периода получено точное значение при определенных ограничениях на разрядное множество.

**Ключевые слова:** скрученная линейная рекуррента, кольцо Галуа, разрядная последовательность

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 2, pp. 19–27 (Russian).

# 1. Introduction. Main results

In what follows, $R = GR(q^d, p^d)$ is a Galois ring, $S = GR(q^{nd}, p^d)$ is a Galois extension of dimension $n$ of $R$ [1]. It is known that the group $\mathrm{Aut}(S/R)$ of automorphisms of $S$ over $R$ is a cyclic group of order $n$ [2]. Let $\sigma$ be a generator of this group and $\check{S} = S^{\sigma}\langle\sigma\rangle$ be a skew group ring of the group $\langle\sigma\rangle$ over the ring $S$, i.e. the set of formal sums $\psi = \sum_{i=0}^{n-1} s_i\sigma^i$, $s_0, \ldots, s_{n-1} \in S$, with natural addition and multiplication, which is introduced using distributive property by the identity $\forall s \in S: \quad \sigma s = \sigma(s)\sigma$.

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

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

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

Following [3], we say that a sequence $v \in S^{\langle 1\rangle}$ is a *skew linear recurrent sequence* (*LRS*) of order $m > 0$ over the ring $S$ if it is an LRS of order $m$ over the module ${}_{\check{S}}S$ [1, 4], i.e. $\Psi(x)v = 0$ for some monic polynomial

$$\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \cdots - \psi_0 \in \check{S}[x] \tag{1.1}$$

of degree $m$, called *characteristic polynomial of LRS* $v$. In other words, the sequence $v$ satisfies the law of recursion

$$\forall i \in \mathbb{N}_0: \quad v(i+m) = \psi_{m-1}(v(i+m-1)) + \cdots + \psi_0(v(i)). \tag{1.2}$$

We denote by $L_S(\Psi)$ the set of all LRS $v$ over $S$ with characteristic polynomial $\Psi$. If $\Psi(x) \in S[x]$, then we say that the sequences from $L_S(\Psi)$ are *classic LRS*.

**Proposition 1 ([3]).** *For any skew LRS $v$ of order $m$ over $S$ there exists a monic polynomial $F(x) \in R[x]$ of degree $mn$ with the following property $v \in L_S(F)$. Moreover, the relations hold:*

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

If $T(v) = \tau$ we say that $v$ is a skew LRS of *maximal period* (*MP LRS*).

The study of skew MP LRS over Galois rings was started in articles [3, 5], where, in particular, the results allowing to construct large classes of such sequences without brute force method was obtained. In papers [6]–[11] skew MP LRS were investigated over finite fields only.

A subset $\mathcal{B} \subset S$ is called *digit set* (*of the ring* $S$), if $0 \in \mathcal{B}$ and for every $a \in S$ there exists a unique element $\varkappa^{\mathcal{B}}(a) \in \mathcal{B}$ such that $\overline{a} = \overline{\varkappa^{\mathcal{B}}(a)}$, where $\overline{a}$ is an image of $a$ under canonical epimorphism $\mu : S \to S/pS$. So, every element $a \in S$ has a unique decomposition

$$a = \varkappa_0^{\mathcal{B}}(a) + p\varkappa_1^{\mathcal{B}}(a) + \ldots + p^{d-1}\varkappa_{d-1}^{\mathcal{B}}(a),\ \varkappa_j^{\mathcal{B}}(a) \in \mathcal{B},\ j \in \overline{0, d-1}. \quad (1.3)$$

We call a function $\varkappa_t^{\mathcal{B}} : S \to \mathcal{B}$ *the* $t$*-th digit function (in the digit set* $\mathcal{B}$*)*. The set $\mathcal{B}$ has a structure of the field of $q^n$ elements with respect to operations $a \oplus b = \varkappa_0^{\mathcal{B}}(a + b), a \odot b = \varkappa_0^{\mathcal{B}}(ab), a, b \in \mathcal{B}$

An important example of a digit set is $p$-adic digit set

$$\Gamma(S) = \{\pi \in S : \pi^{q^n} = \pi\}.$$

For the $t$-th digit function $\varkappa_t^{\Gamma(S)} : S \to \Gamma(S)$ we will use the notation $\gamma_t$.

For any sequence $w \in S^{\langle 1 \rangle}$ there exists a unique tuple $w_0, \ldots, w_{d-1}$ of its *digit sequences* (*in digit set* $\mathcal{B}$), which are defined by the relations

$$w(i) = w_0(i) + pw_1(i) + \ldots + p^{d-1}w_{d-1}(i),\ w_j(i) \in \mathcal{B}, j \in \overline{0, d-1}.$$

**Theorem 2.** *Let* $v \in L_S(\Psi)$ *be a skew MP LRS of order* $m$ *with characteristic polynomial* (1.1) *and* $v_j$ *be its* $j$*-th digit sequence. Then* $v_j$ *is a reversible sequence of period* $T(v_j) = (q^{mn} - 1)p^j$.

For classic MP LRS this result may be found, for example, in [12].

For any sequence $w \in \mathcal{B}^{\langle 1 \rangle}$ we denote by $\mathrm{rank}_{\mathcal{B}} w$ the rank (the degree of minimal polynomial) of the sequence $w$ as LRS over the field $\mathcal{B}$ [13].

**Theorem 3.** *Under conditions of Theorem 2 there exists a tuple* $(k_0, \ldots, k_{d-1})$*, where* $k_j \in \overline{1, n}$, $j \in \overline{0, d-1}$*, such that*

$$\mathrm{rank}_{\mathcal{B}} v_0 = k_0 m, \quad \mathrm{rank}_{\mathcal{B}} v_j \geq k_j m(p^{j-1} + 1),\ j \in \overline{1, d-1}. \quad (1.4)$$

It is known [3] that if $\overline{\Psi}[x] \notin \overline{S}[x]$, then in (1.4) a value $k_0$ is larger than 2. For classic MP LRS all values $k_0, \ldots, k_{d-1}$ in (1.4) are equal to one [12].

## 1.1. The first digit sequence

Let $\Gamma(S) = \{\pi_0 = 0, \ldots, \pi_{q^n-1}\}$. In what follows we assume that if $\mathcal{B}$ is an arbitrary digit set of $S$, $\mathcal{B} = \{\mu_0, \ldots, \mu_{q^n-1}\}$, then $\mu_0 = 0$, $\overline{\mu}_t = \overline{\pi}_t$ for $t = 1, \ldots, q^n - 1$. The following result is valid.

**Lemma 4 ([14]).** *There exists a unique polynomial* $\Lambda_{\mathcal{B}}(x) = \sum\limits_{j=1}^{q^n-1} \lambda_j x^j$ *over* $S$ *such that* $\Lambda(\pi_t) = \mu_t$, $t = 0, \ldots, q^n - 1$. *Moreover,*

$$\Lambda_{\mathcal{B}}(x) = x + p\Lambda^*_{\mathcal{B}}(x), \tag{1.5}$$

*where* $\Lambda^*_{\mathcal{B}}(x) = \sum\limits_{j=1}^{q^n-1} \lambda^*_j x^j \in S[x]$ *is a polynomial uniquely defined modulo* $p^{d-1}$.

We say that (1.5) is an *interpolation polynomial* of the digit set $\mathcal{B}$ and put $L_{\mathcal{B}} = \{l \in \overline{2, q^n - 1} : \lambda_l \not\equiv 0 \,(\mathrm{mod}\, p^2)\}$. Under certain restrictions on this polynomial one can exactly determine a rank of the first digit sequence of the skew linear recurrence of maximal period.

We define a *p-ary decomposition* of number $k \in \mathbb{N}_0$ as an arithmetic sum $w_p(k) = \sum\limits_{s \geq 0} \nu_s(k)$.

Let $v$ be a skew MP LRS of order $m$ over $S$ and $K = GR(q^{nmd}, p^d)$ be an extension of dimension $m$ of the ring $S$. It is known [3] that the $i$-th term $v(i)$ of the sequence $v$ has a representation

$$v(i) = \mathrm{Tr}_S^K \left( \sum\nolimits_{j=0}^{n-1} \varepsilon_j \tilde{\sigma}^j(\vartheta)^i \right) \tag{1.6}$$

for some $\varepsilon_0, \ldots, \varepsilon_{n-1}, \vartheta \in K$, $\mathrm{ord}\vartheta = (q^{mn} - 1)p^{d-1}$, where $\mathrm{Tr}_S^K$ is a trace–function from the ring $K$ onto the ring $S$ and $\tilde{\sigma}$ is a generator of the group $\mathrm{Aut}(K/R)$ [17]. We define

$$W_0 = \{j = \overline{0, n-1} : \ \gamma_0(\varepsilon_j) \neq 0\}, W_1 = \{j = \overline{0, n-1} \setminus W_0 : \ \gamma_1(\varepsilon_j) \neq 0\}.$$

The following results are announced here.

**Theorem 5.** *If* $\Lambda(x) = x + p\Lambda^*(x)$ *is an interpolation polynomial of the digit set* $\mathcal{B}$ *such that*

$$\deg\Lambda(x) \leq q - 1, \tag{1.7}$$

*and skew MP LRS* $v$ (1.6) *satisfies the conditions* $|W_0| = n_0, |W_1| = n_1$, *then*

$$\operatorname{rank}_{\mathcal{B}}\varkappa_1^{\mathcal{B}}(v) = \sum_{l\in L_{\mathcal{B}}}\prod_{s=0}^{r-1}\binom{mn_0+\nu_s(l)-1}{\nu_s(l)} + \binom{mn_0+p-1}{p} + m(n_0+n_1),$$

*in particular,*

$$\operatorname{rank}_{\Gamma(S)}\gamma_1(v) = m(n_0+n_1) + \binom{mn_0+p-1}{p}.$$

For comparison we list the following known result.

**Theorem 6 (**[14]**).** *Let polynomial* (1.5) *be an interpolation polynomial of the digit set* $\mathcal{B}$. *Then the rank of the first digit sequence of the classic MP LRS* $u \in S^{\langle 1\rangle}$ *of order* $m$ *may be calculated by the formula*

$$\operatorname{rank}_{\mathcal{B}}\varkappa_1^{\mathcal{B}}(u) = \sum_{l\in L_{\mathcal{B}}}\prod_{s=0}^{nr-1}\binom{m+\nu_s(l)-1}{\nu_s(l)} + \binom{m+p-1}{p} + m\,. \tag{1.8}$$

**Corollary 7.** *If conditions of Theorem 5 are satisfied and* $n_0 = n$, *then the rank of the first digit sequence of skew MP LRS* $v$ *of order* $m$ *over* $S$ *is equal to the rank of the first digit sequence of classic MP LRS* $u$ *of order* $mn$ *over* $S$.

## 1.2. Proofs

Firstly we prove a series of auxiliary results.

**Proposition 8.** *Let* $v \in L_S(\Psi)$ *be a skew MP LRS of order* $m$ *with a characteristic polynomial* (1.1) *and* $\operatorname{Ann}_{\check{S}[x]}v = \{H(x) \in \check{S}[x] : H(x)v = 0\}$ *be its annihilator in the ring* $\check{S}[x]$. *Then*

$$\operatorname{Ann}_{\check{S}[x]}v = \check{S}[x]\Psi(x). \tag{1.9}$$

**Proof.** Every linear transform $\psi \in \check{S}$ of the module ${}_RS$ induces a linear transform $\overline{\psi} \in \overline{\overline{S}}$ of the space $\overline{R}\overline{S}$ by the rule $\forall\alpha \in S: \quad \overline{\psi}(\overline{\alpha}) = \overline{\psi(\alpha)}$. The correspondence $\psi \to \overline{\psi}$ gives an epimorphism of rings $\check{S} \to \overline{\overline{S}}$ with kernel $p\check{S}$, and canonical isomorphism $\overline{\overline{S}} \cong \check{S}/p\check{S}$ allows to consider $\overline{\psi}$ as an element of

the quotient ring $\check{S}/p\check{S}$, i.e. allows to use the equality $\overline{\psi} = \psi + p\check{S}$. The natural epimorphism $\mu : S \to S/pS$ induces an epimorphism

$$\hat{\mu} : \check{S}[x] \to \overline{\check{S}}[x] \text{ such that } \hat{\mu}\left(\sum\nolimits_{j\geq 0} \psi_j x^j\right) = \sum\nolimits_{j\geq 0} \overline{\psi}_j x^j.$$

In what follows, for the polynomial $\Phi(x) = \sum_{j\geq 0} \varphi_j x^j \in \check{S}[x]$ and for the sequence $u$ over $S$ we put $\overline{\Phi}(x) = \sum_{j\geq 0} \overline{\varphi}_j x^j$, $\overline{u} = w \in \overline{S}^{\langle 1\rangle}$, $w(i) = \overline{u(i)}$.

**Lemma 9.** *The following relation holds:* $\mathrm{Ann}_{\overline{\check{S}}[x]}\overline{v} = \overline{\check{S}}[x]\overline{\Psi}(x)$.

**Proof.** Let us divide with the remainder any polynomial $H(x) \in \mathrm{Ann}_{\overline{\check{S}}[x]}\overline{v}$ from the right side by the polynomial $\overline{\Psi}(x)$ in the ring $\overline{\check{S}}[x]$

$$H(x) = Q(x)\overline{\Psi}(x) + \rho(x), \rho(x) \in \overline{\check{S}}[x],\ \deg\rho(x) < m. \tag{1.10}$$

Multiplying the both sides of equality (1.10) by $\overline{v}$ we obtain $\rho(x)\overline{v} = 0$. The polynomial $\rho(x)$ has the form $\rho(x) = \sum_{j=0}^{m-1} \rho_j x^j$. Since for every $a \in S$ there exists $i = i(a) \in \mathbb{N}_0$ with the property $\overline{v}[i, i+m-1] = (0, \ldots, 0, \overline{a})$, we have from the equality $\rho(x)\overline{v} = 0$ that $\rho_{m-1} = 0$. If $m = 1$, then Lemma is proved. If $m > 1$, then one can analogously show that $\rho_j = 0$ for $j = \overline{0, m-2}$. □

The polynomial $A(x) \in \mathrm{Ann}_{\check{S}[x]}v \setminus \{0\}$ may be represented as

$$A(x) = p^k A_1(x), k \in \overline{0, d-1},\ \overline{A_1}(x) \neq 0,$$

where $A_1(x) \in \check{S}[x]$ is a polynomial uniquely determined modulo $p^{d-k}$. Then $\overline{A_1}(x)\overline{v} = 0$ and by Lemma 9 we obtain

$$A(x) = B(x)\Psi(x) + pC(x),\ \deg C(x) < m. \tag{1.11}$$

If $C(x) \in p^{d-1}\check{S}[x]$, then Theorem is proved. Let $C(x) \notin p^{d-1}\check{S}[x]$. The polynomial $C(x)$ may be represented as

$$C(x) = p^j C_1(x),\ j < d-1,\ C_1(x) \in \check{S}[x],\ \deg C_1(x) < m, \overline{C_1}(x) \neq 0.$$

From the last equation and condition (1.11) we have $\overline{C_1}(x)\overline{v} = 0$, $\overline{C_1}(x) \neq 0$. So, we obtain a contradiction with Lemma 9.

For polynomials $A(x), B(x), C(x) \in \check{S}[x]$ we say that $A(x)$ is right congruent modulo $C(x)$ to $B(x)$, if there exists a polynomial $D(x) \in \check{S}[x]$ such that $A(x) - B(x) = D(x)C(x)$; in this case we will use the notation

$$A(x) \equiv B(x)\ (\mathrm{mod}_{\mathrm{r}} C(x)). \tag{1.12}$$

Note that since the ring $\check{S}[x]$ is noncommutative, we obtain that the equality $A(x) - B(x) = C(x)\tilde{D}(x)$ for some polynomial $\tilde{D}(x) \in \check{S}[x]$ doesn't follow from (1.12). In what follows, $\tau_s = (q^{mn} - 1)p^s, s = \overline{0, d-1}$.

**Lemma 10.** *For any skew MP-polynomial $\Psi(x) \in \check{S}[x]$ of degree $m$ the next conditions are fulfilled*

$$x^{\tau_s} \equiv e + p^{s+1}\Phi^{(s)}(x) \ (\mathrm{mod}_{\mathrm{r}}\Psi(x)), \ s = \overline{0, d-1}, \tag{1.13}$$

*where $\Phi^{(s)}(x) \in \check{S}[x]$, $\deg\Phi^{(s)}(x) < m$, wherein $\overline{\Phi^{(s)}}(x) \neq 0$.*

**Proof.** If $v \in L_S(\Psi)$ is a skew MP LRS of order $m$, then by Proposition 1 there exists an MP-polynomial $F(x) \in R[x]$, $\deg F(x) = mn$ such that $v \in L_S(F)$.

**Lemma 11 ([15]).** *For $s \in \{0, 1, \ldots, d-1\}$ the following relations hold:*

$$x^{\tau_s} \equiv e + p^{s+1}U^{(s)}(x) \ (\mathrm{mod}F), \ U^{(s)}(x) \in R[x], \ \deg U^{(s)}(x) < mn, \ \overline{U^{(s)}}(x) \neq 0.$$

**Proof.** By Proposition 8 there exists a polynomial $\Phi(x) \in \check{S}[x]$ with the property $F(x) = \Phi(x)\Psi(x)$. By Lemma 11 there exist polynomials $H_s(x) \in R[x]$ with the property

$$x^{\tau_s} = e + p^{s+1}U^{(s)}(x) + H_s(x)\Phi(x)\Psi(x). \tag{1.14}$$

Let us divide with the remainder polynomials $U^{(s)}(x)$ from the right side by $\Psi(x)$

$$U^{(s)}(x) = B_s(x)\Psi(x) + \Phi^{(s)}(x), \ \deg\Phi^{(s)}(x) < m. \tag{1.15}$$

Substituting (1.15) in (1.14), we obtain $x^{\tau_s} \equiv e + p^{s+1}\Phi^{(s)}(x) \ (\mathrm{mod}_{\mathrm{r}}\Psi(x))$. Let us show that $\overline{\Phi^{(s)}}(x) \neq 0$. Assume the contrary, that is there exists $t \in \overline{0, d-1}$ with the property $\overline{\Phi^{(t)}}(x) = 0$. Then from relation (1.15) for $s = t$ we get $\overline{U^{(t)}}(x) = \overline{B_t}(x)\overline{\Psi}(x)$. Since polynomials $\overline{U^{(t)}}(x)$, $\overline{F}(x)$ are coprime over $\overline{R}$, we obtain that there exist polynomials $C(x), D(x) \in \overline{R}[x]$ such that $C(x)\overline{U^{(t)}}(x) + D(x)\overline{F}(x) = \overline{e}$. Using the equality $\overline{F}(x) = \overline{\Phi}(x)\overline{\Psi}(x)$, we get $\left(C(x)\overline{B_t}(x) + D(x)\overline{\Phi}(x)\right)\overline{\Psi}(x) = \overline{e}$. The last equality is impossible since $\overline{\Psi}(x)$ is a monic polynomial and $\deg\overline{\Psi}(x) \geq 1$. So we have a contradiction.

**Proof of Theorem 2.** In what follows, for $j \in \mathbb{N}_0$ and $w_1, w_2 \in S^{\langle 1 \rangle}$ we will use the notation

$$w_1 \equiv w_2 (\mathrm{mod}\ p^j) \Longleftrightarrow w_1(i) - w_2(i) \in p^j S, \ i \in \mathbb{N}_0.$$

**Lemma 12.** *Under conditions of Theorem 2 the following relations hold: $T(v_j)|\tau_j, j = \overline{0, d-1}$.*

**Proof.** We will prove this by induction on $j$. For $j = 0$ the sequence $\overline{v}_0$ is a skew MP LRS of order $m$ over the field $\overline{S}$ and has period $T(\overline{v}_0) = T(v_0) = \tau_0$. Assume that conditions $T(v_j)|\tau_j$ are valid for $j < t$ and prove it for $j = t$.

By (1.13) for $j = t$ we obtain $(x^{\tau_t} - e)v = p^{t+1}\Phi^{(t)}(x)v$. On the other hand, by the induction hypothesis

$$(x^{\tau_t} - e)v = \sum_{j=0}^{d-1} p^j (x^{\tau_t} - e)v_j \equiv p^t (x^{\tau_t} - e)v_t \pmod{p^{t+1}}. \tag{1.16}$$

Hence, $(x^{\tau_t} - e)v_t \equiv 0 \pmod{p}$, i.e $T(v_t)|\tau_t$. Lemma is proved.

We will prove Theorem 2 by induction on $j$. As was shown in the proof of Lemma 12, $T(v_0) = \tau_0$. Assume that conditions $T(v_j) = \tau_j$ are valid for $j < t$. By Lemma 12 to prove the Theorem it is sufficient to establish the equality $T(v_{t+1}) > \tau_t$. Let us consider the sequence $(x^{\tau_t} - e)v$ modulo $p^{t+2}$. By Lemma 12

$$p^{t+1}(x^{\tau_t} - e)v_{t+1} \equiv p^{t+1}\Phi^{(t)}(x)v \pmod{p^{t+2}}. \tag{1.17}$$

Using (1.17) we obtain

$$(x^{\tau_t} - \overline{e})\overline{v}_{t+1} = \overline{\Phi^{(t)}}(x)\overline{v}. \tag{1.18}$$

We have $\overline{\Phi^{(t)}}(x) \neq 0, \deg\overline{\Phi^{(t)}}(x) < m$ by Lemma 10 and $\overline{\Phi^{(t)}}(x)\overline{v} \neq 0$ by Lemma 9. So, using equality (1.18) we get $T(v_{t+1}) > \tau_t$. The proof is complete.

**Proof of Theorem 3.** The first equality follows from [3]. By Proposition 1 there exists an MP-polynomial $F(x) \in R[x]$ of degree $mn$ such that $F(x)v = 0$. For every $t \in \overline{0, d-2}$ define a sequence $\omega = \overline{\Phi^{(t)}}(x)\overline{v}$ and consider $\overline{F}(x)\omega$:

$$\overline{F}(x)\omega = \overline{F}(x)\overline{\Phi^{(t)}}(x)\overline{v} = \overline{\Phi^{(t)}}(x)\overline{F}(x)\overline{v} = 0. \tag{1.19}$$

Hence $\omega \in L_{\overline{S}}(\overline{F})$ and $\omega \neq 0$ by Lemma 10. The polynomial $\overline{F}(x)$ has the following canonical decomposition over $\overline{S}$ [16] : $\overline{F}(x) = G_0(x) \cdot \ldots \cdot G_{n-1}(x)$, where $G_0(x), \ldots, G_{n-1}(x)$ are MP-polynomials of degree $m$ over $S$. Hence the equalities $\mathrm{rank}_{\overline{S}}(\omega_t) = k_{t+1}m, 1 \leq k_{t+1} \leq n$, are valid. Let $G(x)$ and $H(x)$ be minimal polynomials of the sequences $\omega_t$ and $\overline{v}_{t+1}$ over $\overline{S}$, correspondingly. If $l \in \mathbb{N}_0$ is a value such that $G(x)^l | H(x), G(x)^{l+1} \nmid H(x)$, then $\mathrm{rank}_{\overline{S}}\overline{v}_{t+1} \geq lk_{t+1}m$. Relation (1.18) may be written in the form $(x^{\tau_0} - \overline{e})^{p^t}\overline{v}_{t+1} = \omega_t$. From the last equality we obtain $G(x) = \frac{H(x)}{(H(x),(x^{\tau_0}-\overline{e})^{p^t})}$ [13]. Since $G(x)|(x^{\tau_0} - \overline{e})$, we have $l = p^t + 1$, hence $\mathrm{rank}_{\mathcal{B}}v_{t+1} = \mathrm{rank}_{\overline{S}}\overline{v}_{t+1} \geq k_{t+1}m(p^t + 1),\ 1 \leq k_{t+1} \leq n$.

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

# References


[1] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., "Linear recurring sequences over rings and modules", *J. Math. Sci.*, **76**:6 (1995), 2793–2915.

[2] Nechaev A.A., "Kerdock code in a cyclic form", *Дискретная математика*, **1**:4 (1989), 123–139 (in Russian).

[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] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyschev V. N., "Linear and polylinear recurring sequences over abelian groups and modules", *J. Math. Sci.*, **102**:6 (2000), 4598–4626.

[5] Goltvanitsa M.A., Nechaev A. A., Zaitsev S. N., "Skew LRS of maximal period over Galois rings", *Математические вопросы криптографии*, **4**:2 (2013), 59–72.

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

[7] Zeng G., Han W., He K., *Word-oriented feedback shift register: σ-LFSR*, http://eprint.iacr.org/2007/114, Cryptology ePrint Archive: Report 2007/114.

[8] Zeng, G., He, K.C., Han,W., "A trinomial type of $\sigma-$LFSR oriented toward software implementation", *Science in China, Series F – Information Sciences*, **50**:3 (2007), 359–372.

[9] Zeng G., Yang Y., Han W., Fan Sh., "Word oriented cascade jump $\sigma$-LFSR", AAECC, 2009, 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.*, **58**:2 (2011), 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 Appl.*, **17**:5 (2011), 461–472.

[12] Kuzmin A.S., Nechaev A. A., "Linear recurring sequences over Galois rings", *Успехи матем. наук*, **48**:1 (1993), 167–168 (in Russian).

[13] Glukhov M. M., Elizarov V. P., Nechaev A. A., *Algebra. Vol. II*, Gelios ARV, 2003 (in Russian).

[14] Kurakin V.L., "The first coordinate sequence of a linear recurrence of maximum period over a Galois ring", *Дискретная математика*, **6**:2 (1994), 88–100 (in Russian).

[15] Kuzmin A.S. Nechaev A.A., "Linear recurring sequences over Galois rings", *Алгебра и Логика*, **3**:2 (1995), 169–189 (in Russian).

[16] Lidl R., Niederreiter H., *Finite Fields, in: Encyclopedia of Mathematics and its Applications*, **20**, Cambridge University Press, 1983.

[17] Nechaev A.A., "Finite Rings with Applications", *Handbook of Algebra*, **5**, eds. M. Hazewinkel, Elsevier B.V., 2008, 213–320.