Math-Net.Ru

Общероссийский математический портал

М. А. Goltvanitsa, Первая разрядная последовательность скрученной линейной рекурренты максимального периода над кольцом Галуа, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 3, 5–18

DOI: <https://doi.org/10.4213/mvk192>

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: 44.207.124.84

26 апреля 2023 г., 16:06:01

**The first digit sequence of skew linear recurrence of
maximal period over Galois ring¹**

M. A. Goltvanitsa

Certification Research Center, LLC, Moscow

Получено 01.III.2015

Abstract. A rank of the first digit sequence of a skew linear recurrence of maximal period is determined under natural conditions on the digit set.

Keywords: skew linear recurrences, Galois ring, digit sequence

**Первая разрядная последовательность скрученной линейной
рекурренты максимального периода над кольцом Галуа**

М. А. Гольтованица

ООО «Центр сертификационных исследований», Москва

Аннотация. Найдены значения ранга первой разрядной последовательности скрученной линейной рекурренты максимального периода при естественных предположениях о разрядном множестве.

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

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 3, pp. 5–18 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

¹ The article was submitted by the Organizing Committee of the Symposium CTCrypt'2015

1. Introduction. Main results

In what follows, $R = GR(q^d, p^d)$ is the Galois ring with $q = p^r$, and $S = GR(q^{nd}, p^d)$ is the Galois extension of dimension n of R [1]. It is known [2] that the group $\text{Aut}(S/R)$ of automorphisms of S over R is a cyclic group of order n . Let σ 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 $\psi = \sum_{i=0}^{n-1} s_i \sigma^i$, $s_0, s_1, \dots, s_{n-1} \in S$, with natural addition and multiplication, which is defined using distributive property by the identity $\sigma s = \sigma(s) \sigma$ for all $s \in S$.

Each element $\psi \in \check{S}$ defines an endomorphism of the module ${}_R S$ such that $\psi(s) = \sum_{i=0}^{n-1} s_i \sigma^i(s)$ for every $s \in S$. So we have the isomorphisms $\check{S} \cong \text{End}({}_R S) \cong R_{n,n}$, where $R_{n,n}$ is 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 $S^{(1)}$ of all sequences over S is a left module over the ring of polynomials $\check{S}[x]$, where a product of the sequence $v \in S^{(1)}$ and the polynomial $A(x) = \sum_{i \geq 0} a_i x^i \in \check{S}[x]$ is defined by the equality

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

Following [3], we say that a sequence $v \in S^{(1)}$ 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 ${}_S S$ [1, 4], i.e. $\Psi(x)v = 0$ for some monic polynomial $\Psi(x) = x^m - \psi_{m-1}x^{m-1} - \dots - \psi_1x - \psi_0 \in \check{S}[x]$ of degree m , called *characteristic polynomial of LRS* v . In other words, the sequence v satisfies the law of recursion

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

Denote by $L_S(\Psi)$ the set of all LRS v over S with characteristic polynomial Ψ . 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 property $v \in L_S(F)$. Moreover, the period $T(v)$ of the sequence v satisfies the inequality $T(v) \leq \tau = (q^{mn} - 1)p^{d-1}$.*

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 had begun in [3, 5], where, in particular, the results allowing to construct large classes of such sequences without brute force method were obtained.

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 $\bar{a} = \varkappa^{\mathcal{B}}(\bar{a})$, where $\bar{a}$ is an image of a under canonical epimorphism $\mu: S \rightarrow S/pS$. So, every element $a \in S$ has a unique decomposition $a = \varkappa_0^{\mathcal{B}}(a) + p\varkappa_1^{\mathcal{B}}(a) + \dots + p^{d-1}\varkappa_{d-1}^{\mathcal{B}}(a)$, $\varkappa_j^{\mathcal{B}}(a) \in \mathcal{B}$, $j \in \overline{0, d-1}$, where the notation $\overline{0, d-1}$ stands for $\{0, 1, \dots, d-1\}$. We call a function $\varkappa_t^{\mathcal{B}}: S \rightarrow \mathcal{B}$ 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

$$a \oplus b = \varkappa_0^{\mathcal{B}}(a + b), \quad a \odot b = \varkappa_0^{\mathcal{B}}(ab), \quad a, b \in \mathcal{B}.$$

An important example of a digit set is $\Gamma(S) = \{\pi \in S: \pi^{q^n} = \pi\}$, called *p-adic digit set*. We use the notation γ_t for the *t-th digit function* $\varkappa_t^{\Gamma(S)}: S \rightarrow \Gamma(S)$.

For any sequence $w \in S^{(1)}$ there exists a unique tuple $w_0, w_1, \dots, w_{d-1}$ of its *digit sequences* (in digit set $\mathcal{B}$) defined by the relations

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

Digit sequences of skew linear recurrences were studied in [6]. For any sequence $w \in \mathcal{B}^{(1)}$ we denote by $\text{rank}_{\mathcal{B}} w$ the rank (the degree of minimal polynomial) of the sequence w as LRS over the field $\mathcal{B}$ [7].

Let $\Gamma(S) = \{\pi_0 = 0, \pi_1, \dots, \pi_{q^n-1}\}$. Further, we assume that if $\mathcal{B}$ is an arbitrary digit set of S , $\mathcal{B} = \{\mu_0, \mu_1, \dots, \mu_{q^n-1}\}$, then $\mu_0 = 0$ and $\bar{\mu}_t = \bar{\pi}_t$ for $t = 1, \dots, q^n - 1$. The following result was obtained in [9].

Lemma 2. *There exists a unique polynomial $\Lambda_{\mathcal{B}}(x) = \lambda_1 x + \lambda_2 x^2 + \dots + \lambda_{q^n-1} x^{q^n-1}$ over S such that $\Lambda_{\mathcal{B}}(\pi_t) = \mu_t$, $t \in \overline{0, q^n-1}$. Further, $\Lambda_{\mathcal{B}}(x) = x + p\Lambda_{\mathcal{B}}^*(x)$, where $\Lambda_{\mathcal{B}}^*(x) = \lambda_1^* x + \lambda_2^* x^2 + \dots + \lambda_{q^n-1}^* x^{q^n-1} \in S[x]$ is a polynomial uniquely defined modulo p^{d-1} .*

We say $\Lambda_{\mathcal{B}}(x)$ is an *interpolation polynomial* of the digit set $\mathcal{B}$ and put $L_{\mathcal{B}} = \{l \in \overline{2, q^n-1}: \lambda_l \not\equiv 0 \pmod{p^2}\}$. Under certain conditions 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 weight* of the number $k = \nu_0(k) + p^1\nu_1(k) + p^2\nu_2(k) + \dots$, where $\nu_s(k) \in \overline{0, p-1}$, as an arithmetic sum $w_p(k) = \nu_0(k) + \nu_1(k) + \nu_2(k) + \dots$.

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 . Denote by $\tilde{\sigma}$ the generator of the group $\text{Aut}(K/R)$ defined as

$$\tilde{\sigma}(\eta) = \gamma_0(\eta)^q + p\gamma_1(\eta)^q + \dots + p^{d-1}\gamma_{d-1}(\eta)^q$$

for each element $\eta \in K$ [2].

It is known [3] that the i -th term $v(i)$ of the sequence v has a representation

$$v(i) = \text{Tr}_S^K \left(\sum_{j=0}^{n-1} \varepsilon_j \tilde{\sigma}^j(\vartheta)^i \right), \quad (1.1)$$

for some $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}, \vartheta \in K$, $\text{ord } \vartheta = (q^{mn} - 1)p^{d-1}$, where Tr_S^K is a trace function from the ring K onto the ring S [10], defined by the rule $\text{Tr}_S^K(\eta) = \sum_{l=0}^{m-1} \tilde{\sigma}^{ln}(\eta)$ for all $\eta \in K$.

In this article we prove the following results announced in [6].

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

Theorem 3. *If $\Lambda(x) = x + p\Lambda^*(x)$ is an interpolation polynomial of the digit set $\mathcal{B}$ such that $\deg \Lambda(x) \leq q - 1$, then for a skew MP LRS v represented by (1.1) such that $|W_0| = n_0, |W_1| = n_1$ the following equality is true:*

$$\text{rank}_{\mathcal{B}\mathcal{X}_1^{\mathcal{B}}}(v) = \sum_{l \in L_{\mathcal{B}}} \prod_{s=0}^{r-1} \binom{mn_0 + \nu_s(l) - 1}{\nu_s(l)} + \binom{mn_0 + p - 1}{p} + m(n_0 + n_1),$$

in particular,

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

For comparison we recall here the following known result.

Theorem 4 ([9]). *Let polynomial $\Lambda_{\mathcal{B}}(x)$ be an interpolation polynomial of the digit set $\mathcal{B}$. Then the rank of the first digit sequence of the classical MP LRS $u \in S^{(1)}$ of order m is equal to*

$$\text{rank}_{\mathcal{B}\mathcal{X}_1^{\mathcal{B}}}(u) = \sum_{l \in L_{\mathcal{B}}} \prod_{s=0}^{nr-1} \binom{m + \nu_s(l) - 1}{\nu_s(l)} + \binom{m + p - 1}{p} + m.$$

Theorem 3 and Theorem 4 imply the following statement.

Corollary 5. *If conditions of Theorem 3 are fulfilled 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 the classical MP LRS u of order mn over S .*

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

2. Proof of Theorem 3

It is known [2] that $\gamma_0(a) \equiv a^{q^n} \pmod{p^2}$ for every $a \in S$. Hence,

$$p \varkappa_1^B(v) \equiv v - \Lambda(v^{q^n}) = v - v^{q^n} - p \lambda_1^* v - p \sum_{l \in L} \lambda_l^* v^l \pmod{p^2}. \quad (2.1)$$

Using (1.1), we have:

$$v(i) = \text{Tr}_S^K(z(i)) \equiv \sum_{k=0}^{m-1} (z_0(i)^{q^{nk}} + p z_1(i)^{q^{nk}}) \pmod{p^2},$$

where $z(i) = \sum_{j=0}^{n-1} \varepsilon_j \sigma^j(\vartheta)^i$, $z_k(i) = \gamma_k(z(i))$, $k = 0, 1$. Hence,

$$\begin{aligned} v(i)^{q^n} &\equiv \left(\sum_{k=0}^{m-1} z_0(i)^{q^{nk}} \right)^{q^n} = \sum_{k=0}^{m-1} z_0(i)^{q^{n(k+1)}} + \\ &+ \sum_{\substack{0 \leq j_0, \dots, j_{m-1} < q^n \\ j_0 + \dots + j_{m-1} = q^n}} \frac{q^n!}{j_0! \cdots j_{m-1}!} z_0(i)^{j_0 + q^n j_1 + \dots + q^{n(m-1)} j_{m-1}} \pmod{p^2}. \end{aligned} \quad (2.2)$$

Since $z_0(i) \in \Gamma(K)$, we obtain $\sum_{k=0}^{m-1} z_0(i)^{q^{n(k+1)}} = \sum_{k=0}^{m-1} z_0(i)^{q^{nk}}$.

All multinomial coefficients in the second sum of (2.2) are divisible by p , so we can write (2.1) in the form

$$p \varkappa_1^B(v)(i) \equiv p u(i) - p w(i) - p \tilde{w}(i) \pmod{p^2},$$

where

$$\begin{aligned} u(i) &= \sum_{k=0}^{m-1} z_1(i)^{q^{nk}} - \lambda_1^* v_0(i), \\ w(i) &= \sum_{\substack{0 \leq j_0, \dots, j_{m-1} < q^n \\ j_0 + \dots + j_{m-1} = q^n}} \frac{q^n! / p}{j_0! \cdots j_{m-1}!} z_0(i)^{j_0 + q^n j_1 + \dots + q^{n(m-1)} j_{m-1}}, \\ \tilde{w}(i) &= \sum_{l \in L} \lambda_l^* v_0(i)^l \end{aligned}$$

and $v_0 = \gamma_0(v)$. The remaining part of the proof is based on lemmas 6–10.

Lemma 6. $\text{rank}_{\Gamma(K)} \gamma_0(u) = m \binom{n_0+p-1}{n_0} + m(n_0+n_1).$

Lemma 7. $\text{rank}_{\Gamma(K)} \gamma_0(w) = \sum_{\substack{0 \leq l_0, \dots, l_{m-1} < p \\ l_0 + \dots + l_{m-1} = p}} \prod_{s=0}^{m-1} \prod_{s=0}^{m-1} \binom{l_s+n_0-1}{l_s}.$

Lemma 8. $\text{rank}_{\Gamma(K)} \gamma_0(\tilde{w}) = \sum_{l \in L} \prod_{s=0}^r \binom{mn_0 + \nu_s(l)-1}{\nu_s(l)}.$

Lemma 9. *Minimal polynomials of the sequences $\gamma_0(u), \gamma_0(w), \gamma_0(\tilde{w})$ are co-prime.*

Lemma 10. $\text{rank}_{\Gamma(K)} \gamma_0(u) + \text{rank}_{\Gamma(K)} \gamma_0(w) = m(n_0+n_1) + \binom{mn_0+p-1}{p}.$

Proof of Lemma 6. It was proved in [11, 3] that $\vartheta_0 \neq 0, \vartheta_1 \neq 0$, so we have

$$\begin{aligned} z(i) &\equiv \sum_{j=0}^{n-1} (\varepsilon_{j0} + p\varepsilon_{j1}) (\vartheta_0^{q^j} + p\vartheta_1^{q^j})^i \equiv \\ &\equiv \sum_{j=0}^{n-1} \varepsilon_{j0} \vartheta_0^{q^j i} + p \left(\sum_{j=0}^{n-1} \varepsilon_{j1} \vartheta_0^{q^j i} + i \sum_{j=0}^{n-1} \varepsilon_{j0} \left(\frac{\vartheta_1}{\vartheta_0} \right)^{q^j} \vartheta_0^{q^j i} \right) \pmod{p^2}, \end{aligned}$$

where $\varepsilon_{jk} = \gamma_k(\varepsilon_j)$. Hence,

$$z_1(i) = \gamma_1 \left(\sum_{j=0}^{n-1} \varepsilon_{j0} \vartheta_0^{q^j i} \right) \oplus \gamma_0 \left(\sum_{j=0}^{n-1} \varepsilon_{j1} \vartheta_0^{q^j i} + i \sum_{j=0}^{n-1} \varepsilon_{j0} \left(\frac{\vartheta_1}{\vartheta_0} \right)^{q^j} \vartheta_0^{q^j i} \right). \quad (2.3)$$

Without loss of generality we can assume $W_0 = \{0, 1, \dots, n_0-1\}$.

Theorem 11 ([12]). *If $a_1, \dots, a_k \in \Gamma(K)$, $\hat{r} = q^{mn}/p$, then*

$$\gamma_1(a_1 + \dots + a_k) \equiv \sum_{\substack{j_0 + \dots + j_k = p \\ 0 \leq j_i < p}} \frac{1}{j_0! \dots j_k!} a_1^{\hat{r}j_1} \dots a_k^{\hat{r}j_k} \pmod{p}. \quad (2.4)$$

Using Theorem 11, we have

$$\begin{aligned}
u(i) &= \sum_{k=0}^{m-1} z_1(i)^{q^{n_k}} - \lambda_1^* v_0(i) \equiv \\
&\equiv \sum_{k=0}^{m-1} \sum_{\substack{s_0+\dots+s_{n_0-1}=p \\ 0 \leq s_k < p}} \frac{\vartheta_0^{\widehat{r}q^{n_k}(s_0+\dots+s_{n_0-1}q^{n_0-1})i}}{s_0! \dots s_{n_0}!} \prod_{j \in W_0} \varepsilon_{j0}^{s_j \widehat{r}q^{n_k}} + \\
&+ \sum_{k=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{j1}^{q^{n_k}} \vartheta_0^{iq^{n_k+j}} + \\
&+ i \sum_{k=0}^{m-1} \sum_{j \in W_0} \varepsilon_{j0}^{q^{n_k}} \left(\frac{\vartheta_1}{\vartheta_0} \right)^{q^{n_k+j}} \vartheta_0^{iq^{n_k+j}} - \\
&- \lambda_1^* \sum_{k=0}^{m-1} \sum_{j \in W_0} \varepsilon_{j0}^{q^{n_k}} \vartheta_0^{iq^{n_k+j}} \pmod{p}. \tag{2.5}
\end{aligned}$$

Let Σ_j be the k -th double sum from (2.5), $j \in \overline{1, 4}$, and let $y(i) = \Sigma_2 + \Sigma_3 + \Sigma_4$, $\widetilde{y} = \Sigma_1$. It is easy to see that the minimal polynomials of the sequences $\gamma_0(y)$ and $\gamma_0(\widetilde{y})$ are coprime and, therefore,

$$\text{rank}_{\Gamma(K)} \gamma_0(y + \widetilde{y}) = \text{rank}_{\Gamma(K)} \gamma_0(y) + \text{rank}_{\Gamma(K)} \gamma_0(\widetilde{y}).$$

Taking into account (2.5) we obtain the decomposition of y into the sum of binomial sequences of the first and second order [7], hence,

$$\text{rang}_{\Gamma(S)} \gamma_0(y) = 2mn_0 + mn_1.$$

Proposition 12 ([6]). *For every $a, b \in \mathbb{N}_0$ the equation $x_1 + \dots + x_a = b$ has $\binom{a+b-1}{b}$ solutions in nonnegative integers.*

Using Proposition 12, we obtain that $\text{rank}_{\Gamma(K)}(u)$ is equal to

$$m \left(\binom{n_0+p-1}{p} - n_0 \right) + 2mn_0 + mn_1 = m \binom{n_0+p-1}{p} + m(n_0+n_1). \quad \square$$

Proof of Lemma 7.

Lemma 13 ([14]). *For every $k \in \mathbb{N}_0$ and every prime p the largest integer i such that $p^i \mid k!$ is equal to $(k - w_p(k))/(p-1)$.*

Therefore, multinomial coefficients in the second sum of (2.2) are divisible by p for every tuple $(j_0, \dots, j_{m-1}) \in \overline{0, q^n - 1}^m$ such that $j_0 + \dots + j_{m-1} = q^n$ and not divisible by p^2 exactly if

$$j_s = \frac{q^n}{p} l_s, \quad l_s \in \overline{0, p-1}, \quad s \in \overline{0, m-1}. \quad (2.6)$$

Let

$$c = c(l_0, \dots, l_{m-1}) = \frac{q^n}{p} (l_0 + q^n l_1 + \dots + q^{n(m-1)} l_{m-1}),$$

then

$$z(i)_0^c \equiv \sum_{\substack{0 \leq k_0, \dots, k_{n_0-1} \leq c \\ k_0 + \dots + k_{n_0-1} = c}} \frac{c!}{k_0! \dots k_{n_0-1}!} \vartheta^{(k_0 + \dots + k_{n_0-1} q^{n_0-1})i} \prod_{j=0}^{n_0-1} (\varepsilon_{j0}^{k_j}) \pmod{p}. \quad (2.7)$$

Theorem 14 ([15, Theorem 4.71]). *If p is a prime number, $N = \sum_{i=0}^I N_i p^i$, $M = \sum_{i=0}^I M_i p^i \in \mathbb{N}_0$, then*

$$\binom{N}{M} \equiv \prod_{i=0}^I \binom{N_i}{M_i} \pmod{p}.$$

By Theorem 14 we conclude that the multinomial coefficient in sum (2.7) is not divisible by p exactly if

$$k_j = \frac{q^n}{p} (l_{0j} + l_{1j} q^n + \dots + l_{m-1,j} q^{n(m-1)}), \quad j \in W_0, \quad (2.8)$$

$$\sum_{j \in W_0} l_{sj} = l_s, \quad l_{sj} \in \overline{0, p-1}, \quad s \in \overline{0, m-1}, \quad l_{sj} \in \mathbb{N}_0.$$

Taking into account (2.8) it is easy to see that elements

$$\vartheta_0^{k_0 + k_1 q + \dots + k_{n_0-1} q^{n_0-1}} = \vartheta_0^{(q^n/p) \sum_{j \in W_0} \sum_{s=0}^{m-1} l_{sj} q^{ns+j}} \quad (2.9)$$

are distinct, because for every $a, b \in \Gamma(K)$ such that $a \neq b$ the inequality $a^{q^n/p} \neq b^{q^n/p}$ is fulfilled and all values $\sum_{j \in W_0} \sum_{s=0}^{m-1} l_{sj} q^{ns+j}$ are distinct and smaller than $\text{ord } \vartheta_0 = q^{mn} - 1$.

So, using (2.6) and (2.7) we get the decomposition of the sequence w into binomial sequences with distinct roots. Finally, taking into account (2.8) and Proposition 12 we obtain the desired result. $\square$

Proof of Lemma 8. For every $l \in L$, using relation

$$v(i)^l \equiv \left(\sum_{k=0}^{m-1} z_0(i)^{q^{n_k}} \right)^l \pmod{p},$$

we get

$$\begin{aligned} v(i)^l \equiv & \sum_{\substack{0 \leq l'_0, \dots, l'_{m-1} \leq l \\ l'_0 + \dots + l'_{m-1} = l}} \sum_{\substack{0 \leq k_0, \dots, k_{n_0-1} \leq c \\ k_0 + \dots + k_{n_0-1} = c}} \frac{l!}{l'_0! \dots l'_{m-1}!} \frac{c!}{k_0! \dots k_{n_0-1}!} \times \\ & \times \prod_{j \in W_0} \varepsilon_{j0}^{k_j} \vartheta_0^{(k_0 + k_1 q + \dots + k_{n_0-1} q^{n_0-1})i} \pmod{p}, \end{aligned} \quad (2.10)$$

where $c = l'_0 + l'_1 q^n + \dots + l'_{m-1} q^{n(m-1)}$. If for nonnegative integers $a_1, \dots, a_k, b$ such that $a_1 + \dots + a_k = b$ the condition $\nu_t(b) = \nu_t(a_1) + \dots + \nu_t(a_k)$ is fulfilled for all $t \in \mathbb{N}_0$, then we will write $b = a_1 \dot{+} \dots \dot{+} a_k$. Taking into account Theorem 14, we get that the product of multinomial coefficients in (2.10) is not divisible by p exactly if

$$l = l'_0 \dot{+} l'_1 \dot{+} \dots \dot{+} l'_{m-1}, \quad c = k_0 \dot{+} k_1 \dot{+} \dots \dot{+} k_{n_0-1}. \quad (2.11)$$

Since $c = l'_0 + l'_1 q^n + \dots + l'_{m-1} q^{n(m-1)}$, combining the second equality in (2.11) and Theorem 14, we get

$$(\forall j \in W_0) \quad k_j = \sum_{s=0}^{m-1} l'_{sj} q^{ns}, \quad \sum_{j \in W_0} l'_{sj} = l'_s \quad \text{for some } l'_s \in \mathbb{N}_0. \quad (2.12)$$

Let us prove that

$$l = l'_{00} \dot{+} l'_{01} \dot{+} \dots \dot{+} l'_{0, n_0-1} \dot{+} \dots \dot{+} l'_{m-1, 0} \dot{+} \dots \dot{+} l'_{m-1, n_0-1}. \quad (2.13)$$

Taking into account the inequality $l \leq q-1$, it suffices to prove that

$$\nu_b(l) = \sum_{j \in W_0} \sum_{s=0}^{m-1} \nu_b(l'_{sj}) \quad \text{for all } b \in \overline{0, r-1}.$$

It is easy to see that the condition $\nu_{arn+b}(c) = \nu_b(l'_a)$ holds true for all $a, b \in \mathbb{N}_0$, $a < m$, $b < rn$. On the other hand, using (2.11), (2.12) we have

$$\nu_{arn+b}(c) = \sum_{j=0}^{n_0-1} \nu_{arn+b}(k_j) = \sum_{j=0}^{n_0-1} \nu_b(l'_{aj}).$$

So, using the first equality in (2.11), we obtain $\nu_b(l) = \sum_{j \in W_0} \sum_{s=0}^{m-1} \nu_b(l'_{sj})$ for all $a \in \overline{0, m-1}$, $b \in \overline{0, rn-1}$. Hence (2.13) is proved.

It is easy to see that the condition (2.11) follows from conditions (2.13), (2.12). So conditions (2.13) and (2.11) are equivalent. Hence, the number of non-zero terms in (2.10) is equal to the number of decompositions of l in the form (2.13). Using Proposition 12, we obtain that this number is equal to

$$\prod_{s=0}^{r-1} \binom{mn_0 + \nu_s(l) - 1}{\nu_s(l)}.$$

Note that (2.10) is the decomposition of v into the sum of binomial sequences with roots of the form

$$\vartheta_0^{\sum_{s=0}^{m-1} \sum_{j \in W_0} l'_{sj} q^{ns+j}}. \quad (2.14)$$

Since $l'_{sj} \leq l \leq q-1$ and $\text{ord } \vartheta_0 = q^{mn} - 1$, we obtain that all elements (2.14) are distinct. So, the following equality is fulfilled

$$\text{rank}_{\Gamma(S)} \gamma_0(v^l) = \prod_{s=0}^{r-1} \binom{mn_0 + \nu_s(l) - 1}{\nu_s(l)}.$$

Finally, note that for distinct $l_1, l_2 \in L$ the minimal polynomials of the sequences $\gamma_0(v^{l_1})$ and $\gamma_0(v^{l_2})$ are coprime. $\square$

Proof of Lemma 9. Let us prove that minimal polynomials of the sequences $\gamma_0(u)$ and $\gamma_0(w)$ are coprime. It suffices to show that the set of roots of binomial sequences in decomposition (2.5) does not intersect with the set of elements (2.9). Assume the contrary: for some $k \in \overline{0, m-1}$, $t \in \overline{0, n-1}$ one of the equalities is fulfilled

$$\vartheta_0^{\widehat{r} q^{nk} (b_0 + b_1 q + \dots + b_{n_0-1} q^{n_0-1})} = \vartheta_0^{(q^n/p) \sum_{j \in W_0} \sum_{s=0}^{m-1} l_{sj} q^{ns+j}}, \quad (2.15)$$

$$\vartheta_0^{q^{nk+t}} = \vartheta_0^{(q^n/p) \sum_{j \in W_0} \sum_{s=0}^{m-1} l_{sj} q^{ns+j}}, \quad (2.16)$$

where $\widehat{r} = \frac{q^{mn}}{p}$, l_{sj} satisfy condition (2.8), and $\sum_{j \in W_0} b_j = p, 0 \leq b_j < p$.

Let us show that equality (2.15) is not fulfilled (For equality (2.16) the proof is analogous). If $k = 0$, then condition (2.15) is equivalent to the condition

$$\vartheta_0^{q^{n(m-1)} (b_0 + b_1 q + \dots + b_{n_0-1} q^{n_0-1})} = \vartheta_0^{\sum_{j=0}^{n_0-1} \sum_{s=0}^{m-1} l_{sj} q^{ns+j}}. \quad (2.17)$$

Using (2.8), we have

$$\sum_{j \in W_0} l_{sj} = l_s, \quad l_{sj} \in \overline{0, p-1}, \quad s \in \overline{0, m-1}, \quad \sum_{s=0}^{m-1} l_s = p, \quad 0 \leq l_s < p,$$

therefore, there exist $0 \leq s_1 \leq m-1$, $0 \leq s_2 \leq m-1$, $s_1 \neq s_2$ such that $l_{s_1} \neq 0$, $l_{s_2} \neq 0$. Hence, there exist $j_1, j_2 \in W_0$ such that $l_{s_1 j_1} \neq 0$, $l_{s_2 j_1} \neq 0$. So, equation (2.17) is not fulfilled, since ϑ_0 enters into the left- and right-hand sides of (2.17) with different exponents which are smaller than $\text{ord } \vartheta_0$.

If $0 < k \leq m-1$, then the condition (2.15) is equivalent to the condition

$$\vartheta_0^{q^{n(k-1)}(b_0 + b_1 q + \dots + b_{n_0-1} q^{n_0-1})} = \vartheta_0^{\sum_{j=0}^{n_0-1} \sum_{s=0}^{m-1} l_{sj} q^{n s+j}}. \quad (2.18)$$

In this case the proof is analogous to the proof in the case $k = 0$.

Let us show that minimal polynomials of the sequences $\gamma_0(w)$ and $\gamma_0(\tilde{w})$ are coprime. It suffices to show that the set of elements of the form (2.9) does not intersect with the set of elements of the form (2.14). Assume the contrary: for some tuple l_{sj} , where $s \in \overline{0, m-1}, j \in W_0$ such that

$$\sum_{j \in W} \sum_{s=0}^{m-1} l_{sj} = p, \quad 0 \leq l_{sj} < p,$$

and l of the form (2.13) the following equality is fulfilled

$$\vartheta_0^{\sum_{j \in W_0} \sum_{s=0}^{m-1} l'_{sj} q^{n s+j}} = \vartheta_0^{(q^n/p) \sum_{j \in W_0} \sum_{s=0}^{m-1} l_{sj} q^{n s+j}}. \quad (2.19)$$

Denote

$$\begin{aligned} a &\equiv p \sum_{j \in W_0} \sum_{s=0}^{m-1} l'_{sj} q^{n s+j} \pmod{(q^{mn}-1)}, \\ b &\equiv q^n \sum_{j \in W_0} \sum_{s=0}^{m-1} l_{sj} q^{n s+j} \pmod{(q^{mn}-1)}, \quad 0 \leq a, b < q^{mn}-1. \end{aligned}$$

Equality (2.19) is equivalent to the condition $a = b$. Now we consider two cases: $q = p$ and $q > p$.

If $q = p$, then

$$w_p(a) = l \leq q-1 = p-1 < p, \quad w_p(b) = p.$$

So, $a \neq b$ and condition (2.19) is not fulfilled. This is a contradiction.

Let us consider the case $q > p$, i. e. $r = \log_p q > 1$. In this case there are two possible sub-cases. If

$$(\exists s_0 \in \overline{0, m-1}, j_0 \in W_0) \quad p^{r-1} \nmid l'_{s_0 j_0} \neq 0, \quad (2.20)$$

then there exists $t > 0$ such that

$$r \nmid t, \quad \nu_t(a) \neq 0. \quad (2.21)$$

It is easy to see that condition (2.21) is not fulfilled for b . This is a contradiction. If condition (2.20) is not valid, i. e.

$$(\forall s \in \overline{0, m-1}, j \in W_0) \quad p^{r-1} \mid l'_{s j}, \quad (2.22)$$

then $l'_{s j} = p^{r-1} h_{s j}$. Taking into account (2.13), we obtain that

$$w_p(a) = \sum_{j \in W_0} \sum_{s=0}^{m-1} h_{s j} < p.$$

On the other hand, $w_p(b) = p$. Hence, $a \neq b$. This is a contradiction. So, minimal polynomials of the sequences $\gamma_0(w)$ and $\gamma_0(\tilde{w})$ are coprime. The proof of the fact that minimal polynomials of the sequences $\gamma_0(u)$ and $\gamma_0(\tilde{w})$ are coprime is analogous. $\square$

Proof of Lemma 10. Combining Lemma 6 with Lemma 7, we get

$$\begin{aligned} & \text{rank}_{\Gamma(K)} \gamma_0(u) + \text{rank}_{\Gamma(K)} \gamma_0(v) = \\ & = m \binom{n_0 + p - 1}{n_0} + m(n_0 + n_1) + \sum_{\substack{0 \leq l_0, \dots, l_{m-1} < p \\ l_0 + \dots + l_{m-1} = p}} \prod_{s=0}^{m-1} \binom{l_s + n_0 - 1}{l_s} = \\ & = \sum_{\substack{0 \leq l_0, \dots, l_{m-1} \leq p \\ l_0 + \dots + l_{m-1} = p}} \prod_{s=0}^{m-1} \binom{l_s + n_0 - 1}{l_s} + m(n_0 + n_1). \end{aligned}$$

Using Proposition 12, we have

$$\sum_{\substack{0 \leq l_0, \dots, l_{m-1} \leq p \\ l_0 + \dots + l_{m-1} = p}} \prod_{s=0}^{m-1} \binom{l_s + n_0 - 1}{l_s} = \binom{mn_0 + p - 1}{p}.$$

So, Lemma 10 is proved. This completes the proof of Theorem 3. $\square$

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”, *Diskretnaya Matematika*, **1**:4 (1989), 123–139 (in Russian); Engl. transl., *Discrete Math. Appl.*, **1**:4 (1991), 365–384.
- [3] Goltvanitsa M.A., Nechaev A.A., Zaitsev S.N., “Skew linear recurring sequences of maximal period over Galois rings”, *Fundamental. Prikl. Matem.*, **17**:3 (2011/12), 5–23 (in Russian); Engl. transl., *J. Math. Sci.*, **187**:2 (2012), 115–128.
- [4] Kurakin V.L., Mikhalev A.V., Nechaev A.A., Tsypyshev V.N., “Linear and polynomial 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”, *Matematicheskie voprosy kriptografii (Math. Aspects Cryptogr.)*, **4**:2 (2013), 59–73 (in Russian).
- [6] Goltvanitsa M.A., “Digit sequences of skew linear recurrences of maximal period over Galois rings”, *Matematicheskie voprosy kriptografii (Math. Aspects Cryptogr.)*, **6**:2 (2015), 189–197 (in Russian).
- [7] Glukhov M.M., Elizarov V.P., Nechaev A.A., *Algebra. Book II*: Gelios ARV, 2003 (in Russian).
- [8] Kuzmin A.S., Nechaev A.A., “Linear recurring sequences over Galois rings”, *Uspekhi Matem. Nauk*, **48**:1 (1993), 167–168 (in Russian); Engl. transl., *Russian Math. Surveys*, **48**:1 (1993), 171–172.
- [9] Kurakin V.L., “The first coordinate sequence of a linear recurrence of maximum period over a Galois ring”, *Diskretnaya Matematika*, **6**:2 (1994), 88–100 (in Russian); Engl. transl., *Discrete Math. Appl.*, **4**:2 (1994), 129–141.
- [10] Nechaev A.A., “Finite Rings with Applications”. In: “*Handbook of Algebra*”, **5** ed. M. Hazewinkel: Elsevier B.V., 2008, 213–320.
- [11] Nechaev A.A., “Cycle types of linear substitutions over finite commutative rings”, *Matem. Sb.*, **184**:3 (1993), 21–56 (in Russian); Engl. transl., *Russian Academy of Sciences. Sbornik. Mathematics*, **78**:2 (1994), 283–311.
- [12] Kurakin V.L., “The first digit carry function in the Galois ring”, *Diskretnaya Matematika*, **24**:2 (2012), 21–36 (in Russian); Engl. transl., *Discrete Math. Appl.*, **22**:3 (2012), 241–259.
- [13] Sachkov V.N., *Introduction to Combinatorial Methods in Discrete Mathematics*, Moscow: Nauka, 1982 (in Russian), 384 p.

- [14] Lidl R., Niederreiter H., *Finite Fields, in: Encyclopedia of Mathematics and its Applications*, **20**: Cambridge Univ. Press, 1983; Russian transl. , Moscow: Mir Publishers, 1988.
- [15] Berlecamp E., *Algebraic Coding Theory*, New York: McGraw-Hill Inc., 1968; Russian transl., Moscow: Mir Publishers, 1971.