Linear Complexity of Designs based on Coordinate Sequences of LRS and on Digital Sequences of Matrix/Skew LRS Coordinate Sequences over Galois Ring*

Tsypyschev V.N.†

Abstract

This article continues investigation of ways to obtain pseudo-random sequences over Galois field via generating LRS over Galois ring and complication it.

Previous work is available at http://eprint.iacr.org/2016/212

In this work we provide low rank estimations for sequences generated by two different designs based on coordinate sequences of linear recurrent sequences (LRS) of maximal period (MP) over Galois ring $R = GR(p^n, r)$, $p \geq 5$, $r \geq 2$, with numbers s such that $s = kr+2$, $k \in \mathbb{N}_0$, and based on digital sequences of coordinate sequences of matrix/skew MP LRS over such Galois rings.

Keywords: linear recurrent sequence, linear complexity/rank estimations, pseudo-random sequences, matrix linear recurrent sequence, matrix linear congruent generator, skew linear recurrent sequence.

1 Introduction

Here we continue investigation of linear complexity properties of different ways to generate pseudo-random sequences over Galois field wich essentially involves linear recurrences over Galois ring as an intermediate sequence for further complication.

On IACR ePrint Archive we have published two articles devoted to this theme [22, 23]. So we have no need to cite here well-known facts of linear recurrences over Galois ring theory from [17, 18, 15, 16, 14, 10] and explain notification. Also we have not to explain properties well-generated pseudo-random sequance has to obtain [3].

Only which we have to cite here for our convenience is basic result of works [22, 23].

*This work is dedicated to the memory of A.S.Kuzmin, V.L.Kurakin and A.A.Nechaev

†Moscow Technological University MIREA

Theorem 1.1. Let $R = GR(p^n, r)$ be a non-trivial Galois ring, $q = p^r$, $p \geq 5$, $r \geq 2$, $F(x)$ be a polynomial of maximal period and degree m over ring R, u be a non-zero modulo pR sequence with characteristic polynomial $F(x)$, $S = GR(p^n, rm)$ be a Galois extension of R, θ be a root of $F(x)$ in S, $\xi \in S$ be under condition

$$u(i) = \mathrm{Tr}_R^S \left(\xi \cdot \theta^i\right).$$

Let $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$. Let's denote by $\mathcal{F}(x) = \gamma_0(F(x))$.

$$H(x) = \prod_{\substack{\vec{\lambda} \in \mathcal{I}(m,p), \\ \vec{\zeta} \in \mathcal{I}(m,p-1)}} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l + p\zeta_l)}\right), \tag{1.1}$$

$$Z(x) = \prod_{\vec{\zeta} \in \mathcal{I}(m,p)} \left(x \ominus \theta_0^{\sum\limits_{l=0}^{m-1} p^{rm+rl-1} \cdot \zeta_l}\right). \tag{1.2}$$

Then for every natural $s > 2$ such that

$$s \equiv 2 \pmod r, \tag{1.3}$$

this divisibility holds:

$$\mathcal{F}(x)^{p^{s-1}+1} \cdot H(x)^{p^{s-1}} \Big| \, m_s(x), \tag{1.4}$$

and this inequality holds:

$$m(p^{s-1} + 1) + p^{s-1} \cdot \left\{ \begin{matrix} m \\ p \end{matrix} \right\} \cdot \left\{ \begin{matrix} m \\ p-1 \end{matrix} \right\} \leq \operatorname{rank} u_s. \tag{1.5}$$

Besides that, if $\xi_1 \neq 0$ and additional conditions take place:

$$\forall \vec{\zeta} \in \mathcal{I}(m,p) \quad \sum_{\kappa = \overline{0,m-1} \,:\, \zeta_\kappa > 0}\!\!\!\!\oplus \quad (\xi_0^{-1} \xi_1)^{p^{rm+r\kappa-1}} \neq 0 \tag{1.6}$$

and

$$\forall \vec{\zeta} \in \mathcal{I}(m,p) \quad \sum_{l = \overline{0,m-1} \,:\, \zeta_l > 0}\!\!\!\!\oplus \quad \gamma_0 \left(\frac{\zeta_l}{\prod_{\kappa=0}^{m-1} \zeta_\kappa!} \right) (\theta_0^{-1} \theta_1)^{\sum_{\kappa=0}^{m-1} \zeta_\kappa p^{rm+r\kappa-1} - p^{rm+rl-1}} \neq 0, \tag{1.7}$$

then for previous s this divisibility holds:

$$\mathcal{F}(x)^{p^{s-1}+1} \cdot H(x)^{p^{s-1}} \cdot Z(x)^{p^{s-1}} \Big| \, m_s(x), \tag{1.8}$$

and this inequality takes place:

$$m(p^{s-1} + 1) + p^{s-1} \cdot \left\{ \begin{matrix} m \\ p \end{matrix} \right\} \cdot \left\{ \begin{matrix} m \\ p-1 \end{matrix} \right\} + p^{s-1} \cdot \left\{ \begin{matrix} m \\ p \end{matrix} \right\} \leq \operatorname{rank} u_s. \tag{1.9}$$

$\square$

Let $M, w \in \mathbb{N}$. Let's denote by $\mathcal{I}(M, w)$ the set of vectors $\vec{\jmath} = (j_1, \ldots, j_M)$, $0 \le j_l \le p-1$, $l = \overline{1, M}$, with property: $\sum_{l=1}^{M} j_l = w$, and by $\left\{ {M \atop w} \right\}$ let's denote cardinality of the set $\mathcal{I}(M, w)$. Let's note that $\left\{ {M \atop w} \right\}$ is a number of placements of w indistinguishable balls in M different boxes under condition that in every box may be placed not more than $(p-1)$ balls.

These equalities are true [19, p.215]:

$$\left\{ {M \atop w} \right\} = \sum_{s=0}^{\min\{w,(M-w)/p\}} (-1)^s \binom{w}{s} \binom{M + w - ps - 1}{M - 1}, \tag{1.10}$$

if $0 \le w \le M(p-1)$, and

$$\left\{ {M \atop w} \right\} = 0 \tag{1.11}$$

in other case.

Further we shall suppose that vectors $\vec{\jmath}$ constituting the set $\mathcal{I}(M, w)$ are ordered ascending in lexicographical order.

Let's note here that

$$\deg H(x) = \left\{ {m \atop p} \right\} \cdot \left\{ {m \atop p-1} \right\},$$

$$\deg Z(x) = \left\{ {m \atop p} \right\}.$$

Further we shall investigate linear complexity of such extrapolations of cryptologic design investigated previously in [22, 23]:

$$\begin{array}{cccccc}
u^{(1)}(i) & \mapsto & v^{(1)}(i) = \gamma_s\left(u^{(1)}(i)\right) & \searrow & & \\
\vdots & \vdots & \vdots & \vdots & & \\
u^{(k)}(i) & \mapsto & v^{(k)}(i) = \gamma_s\left(u^{(k)}(i)\right) & \rightarrow & v(i) = \prod_{\kappa=1}^{d} v^{(\kappa)}(i), i \in \mathbb{N}_0 & \\
\vdots & \vdots & \vdots & \vdots & & \\
u^{(d)}(i) & \mapsto & v^{(d)}(i) = \gamma_s\left(u^{(d)}(i)\right) & \nearrow & &
\end{array} \tag{1.12}$$

Here s is a constant parameter, $u^{(1)}, \ldots, u^{(d)}$ are linearly independent MP LRS over R with common characteristic Galois polynomial $F(x)$ of maximal period. Let's make accent on the fact that sequence v is over Galois field $\Gamma(R) = GF(p^r)$.

For sequence v we provide divisors of its characteristic polynomial and investigate its linear complexity estimates and periodical properties.

As a next step we shall investigate this Scheme of pseudo-random sequence generating:

$$
\begin{array}{ccc}
\vec{U}(i) = (u_1(i), \ldots, u_m(i)) & \mapsto & \vec{W}(i) = (w_1(i) = \gamma_s(u_1(i)), \ldots, w_m(i) = \gamma_s(u_m(i))) \\
 & & \downarrow \\
 & & w(i) = \prod\limits_{\kappa=1}^{m} w_\kappa(i), i \in \mathbb{N}_0
\end{array}
\tag{1.13}
$$

Here, as previously, s is a constant parameter of the Scheme 1.13, $\vec{U} = (u_1, \ldots, u_m)$ is a ordered set of sequences, satisfying the rule:

$$
\vec{U}(i+1) = A \cdot \vec{U}(i), i \in \mathbb{N}_0, \tag{1.14}
$$

where $A \in R_{m,m}$ — matrix over R of m rows and of m columns. For our purposes we shall assume that the period of A is maximal and is equal to $\mathrm{T}(A) = (p^{rm} - 1) \cdot p^{n-1}$. Also let's emphasize that sequence w is over Galois field $\Gamma(R) = GF(p^r)$.

Sequence 1.14 may be treated as partial form of a matrix linear recurrent sequence in terms of [13], or as a partial form of matrix linear congruent generator in terms of [20], or a simply skew LRS in terms of [2]. Let's note also that sometimes sequences $u_\kappa, \kappa = \overline{1,m}$ are called coordinate sequences of matrix LRS, and sequences $w_\kappa, \kappa = \overline{1,m}$ are called digital sequences of $u_\kappa, \kappa = \overline{1,m}$.

For sequence w we shall provide divisors of its minimal polynomial, low estimates of its linear complexity, its periodical properties.

Let's note that the complication function of cryptographic design of article [23] is injective compressing map, as it proved in [12]. For designs 1.12 and 1.13 this question is still open.

2 Properties of Design 1.12

Before we shall investigate Design 1.12, we have to remind some old results of Zierler and Mills.

For an arbitrary ring R by $L_R(F)$ we denote the set of all linear recurrences with a characteristic polynomial $F(x)$. By $L_R(F_1) \cdots L_R(F_k)$ we denote the linear span of the set of all recurrences obtained as a point-wise products of linear recurrences from $L_R(F_1)$,..., $L_R(F_k)$. From [24] we know that if $P = GF(q)$ is a finite field, $F_1(x), \ldots, F_k(x)$, is a set of monic polynomials over P then

$$
L_P(F_1) \cdots L_P(F_k) = L_P(H), \tag{2.1}
$$

where polynomial $H(x) \in P[x]$ is described in this way: Let

$$
F_s(x) = \prod_{j_s=1}^{l_s} G_{j_s}^{(s)}(x)^{b_{j_s}^{(s)}}, s = \overline{1,k} \tag{2.2}
$$

is a canonical decomposition, and for an

$$a^{(t)} - 1 = \sum_{\nu \geq 0} \zeta_\nu^{(t)} p^\nu \in \mathbb{N}_0, 0 \leq \zeta_\nu < p, t = \overline{1,k}, \tag{2.3}$$

we denote

$$\bigvee_{t=1}^{k} a^{(t)} = p^\lambda + \sum_{\nu \geq \lambda} (\sum_{t=1}^{k} \zeta_\nu^{(t)}) p^\nu, \tag{2.4}$$

where

$$\lambda = \min\{\lambda \geq 0 \mid \forall \nu \geq \lambda \sum_{t=1}^{k} \zeta_\nu^{(t)} < p\}. \tag{2.5}$$

Besides that, for polynomials $F(x), G(x), \ldots, H(x) \in P[x]$ by $F(x) \vee G(x) \vee \cdots \vee H(x)$ we denote polynomial with the set of roots is equal to the set of all distinct products of roots of polynomials $F(x), G(x), \ldots, H(x)$ in theirs common splitting field. In this case $F(x) \vee G(x) \vee \cdots \vee H(x) \in P[x]$.

Then

$$H(x) = \operatorname*{LCM}_{j_s \in \overline{1,l_s}, s=\overline{1,k}} \left\{ \left(\bigvee_{s=1}^{k} G_{j_s}^{(s)}(x) \right)^{\bigvee_{s=1}^{k} b_{j_s}^{(s)}} \right\}. \tag{2.6}$$

Let's denote by

$$\bigvee_\alpha G(x) = \underbrace{G(x) \vee \cdots \vee G(x)}_{\alpha \ times}$$

and by

$$\bigvee_\alpha a = \underbrace{a \vee \cdots \vee a}_{\alpha \ times}$$

Before we start investigate divisors of $m_v(x)$ we have to provide these Lemmas:

Lemma 2.1.

$$\bigvee_\alpha (p^{s-1} + 1) = \begin{cases} (\alpha + 1)p^{s-1}, \ 1 \leq \alpha \leq p - 2; \\ p^s, \ p - 1 \leq \alpha \end{cases} \tag{2.7}$$

□

and

Lemma 2.2.

$$\bigvee_\beta p^{s-1} = p^{s-1}. \tag{2.8}$$

□

and

Lemma 2.3.

$$\underbrace{p^{s-1} + 1 \vee \cdots \vee p^{s-1} + 1}_{\alpha \ times} \vee \underbrace{p^{s-1} \vee \cdots \vee p^{s-1}}_{d - \alpha \ times} = \begin{cases} (\alpha + 1)p^{s-1}, \ 1 \leq \alpha \leq p - 2; \\ p^s, \ p - 1 \leq \alpha \end{cases} \tag{2.9}$$

$\square$

Let's remember that

$$\mathcal{F}(x) = \prod_{j=0}^{m-1} \left(x \ominus \theta_0^{p^{rj}} \right),$$

and

$$H(x) = \prod_{\substack{\vec{\lambda} \in \mathcal{I}(m,p), \\ \vec{\zeta} \in \mathcal{I}(m,p-1)}} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l + p\zeta_l)} \right),$$

as is defined in (1.1).

Lemma 2.4. Let's denote by

$$\mathcal{F}^{(d)}(x) = \prod_{j=0}^{m-1} (x \ominus \theta_0^{dp^{rj}}),$$

$$\mathcal{F}^{(d-1)}(x) = \prod_{\substack{\{j_1,\dots,j_{d-1}\} \subset \overline{0,m-1},\ j_1 < \dots < j_{d-1} \\ \delta_1,\dots,\delta_{d-1} \in \overline{0,d-1}:\ \delta_1 + \dots + \delta_{d-1} = d}} (x \ominus \theta_0^{\delta_1 p^{rj_1} + \dots + \delta_{d-1} p^{rj_{d-1}}}),$$

$$\dots$$

$$\mathcal{F}^{(1)}(x) = \prod_{j_1 < \dots < j_d} (x \ominus \theta_0^{p^{rj_1} + \dots + p^{rj_d}}),$$

$$W^{(\alpha)}(x) =$$

$$= \prod_{\substack{j_1 < \dots < j_\alpha \in \overline{0,m-1} \\ \vec{\lambda}^{(1)} < \dots < \vec{\lambda}^{(\beta)} \in \mathcal{I}(m,p), \\ \vec{\zeta}^{(1)} < \dots < \vec{\zeta}^{(\beta)} \in \mathcal{I}(m,p-1),\ \beta = d-\alpha}} \left(x \ominus \theta_0^{p^{rj_1} + \dots + p^{rj_\alpha} + \sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(1)} + p\zeta_l^{(1)}) + \dots + \sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(\beta)} + p\zeta_l^{(\beta)})} \right),$$

$\alpha = \overline{1, d-1}$, and

$$H^{(d)}(x) = \prod_{\substack{\vec{\lambda} \in \mathcal{I}(m,p), \\ \vec{\zeta} \in \mathcal{I}(m,p-1)}} \left(x \ominus \theta_0^{d \sum_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l + p\zeta_l)} \right),$$

$$H^{(d-1)}(x) = \prod_{\substack{\vec{\lambda}^{(1)} < \dots < \vec{\lambda}^{(d-1)} \in \mathcal{I}(m,p), \\ \vec{\zeta}^{(1)} < \dots < \vec{\zeta}^{(d-1)} \in \mathcal{I}(m,p-1), \\ \delta_1,\dots,\delta_{d-1} \in \overline{0,d}:\ \delta_1 + \dots + \delta_{d-1} = d}} (x \ominus$$

$$\left. \ominus \theta_0^{\delta_1 \sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(1)} + p\zeta_l^{(1)}) + \dots + \delta_{(d-1)} \sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(d-1)} + p\zeta_l^{d-1})} \right),$$

$$\dots$$

$$H^{(1)}(x) = \prod_{\substack{\vec{\lambda}^{(1)} < \cdots < \vec{\lambda}^{(d)} \in \mathcal{I}(m,p), \\ \vec{\zeta}^{(1)} < \cdots < \vec{\zeta}^{(d)} \in \mathcal{I}(m,p-1),}} \left(x \ominus \theta_0^{\sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(1)} + p\zeta_l^{(1)}) + \cdots + \sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(d)} + p\zeta_l^{(d)})} \right).$$

Then

$$\deg \mathcal{F}^{(d)}(x) = m, \ \deg \mathcal{F}^{(\alpha)}(x) = \binom{m}{\alpha} \cdot \binom{d-1}{\alpha-1}, \ \alpha = \overline{1, d-1},$$

$$\deg W^{(\alpha)}(x) = \binom{m}{\alpha} \cdot \binom{\left\{ {m \atop p} \right\}}{d-\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{d-\alpha}, \ \alpha = \overline{1, d-1},$$

$$\deg H^{(d)}(x) = \left\{ {m \atop p} \right\} \left\{ {m \atop p-1} \right\},$$

$$\deg H^{(\alpha)}(x) = \binom{\left\{ {m \atop p} \right\}}{\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{\alpha} \cdot \binom{d-1}{\alpha-1}, \ \alpha = \overline{1, d-1}.$$

$\square$

Theorem 2.5. Let $R = GR(p^n, r)$ be a non-trivial Galois ring, $q = p^r$, $p \geq 5$, $r \geq 2$, $F(x)$ be a polynomial of maximal period and degree m over ring R, $u^{(1)}, \ldots, u^{(d)}$ are non-zero modulo pR sequences with characteristic polynomial $F(x)$, $d \leq m$, for $\kappa \in \overline{1, d}$ $v_\kappa = \gamma_s(u^{(\kappa)})$, $s \equiv 2 \pmod r$,

$$v = \prod_{\kappa=1}^{d} v_\kappa,$$

$S = GR(p^n, rm)$ be a Galois extension of R, θ be a root of $F(x)$ in S, polynomial $H(x)$ is defined as in (1.1), $\mathcal{F}(x) = \gamma_0(F(x))$.

Then

$$\begin{aligned} &\left(\prod_{\alpha=1}^{p-2} \mathcal{F}^{(\alpha)}(x)^{(\alpha+1)p^{s-1}} \cdot \prod_{\alpha=p-1}^{d} \mathcal{F}^{(\alpha)}(x)^{p^s} \cdot \prod_{\alpha=1}^{p-2} W^{(\alpha)}(x)^{(\alpha+1)p^{s-1}} \cdot \right. \\ &\left. \prod_{\alpha=p-1}^{d-1} W^{(\alpha)}(x)^{p^s} \cdot \prod_{\alpha=1}^{d} H^{(\alpha)}(x)^{p^{s-1}} \right) \Bigg| \ m_v(x) \end{aligned} \tag{2.10}$$

and

$$\begin{aligned} &m + \sum_{\alpha=1}^{p-2} (\alpha+1) p^{s-1} \binom{m}{\alpha} \cdot \binom{d-1}{\alpha-1} + \sum_{\alpha=p-1}^{d-1} p^s \cdot \binom{m}{\alpha} \cdot \binom{d-1}{\alpha-1} + \\ &+ \sum_{\alpha=1}^{p-2} (\alpha+1) p^{s-1} \cdot \binom{m}{\alpha} \cdot \binom{\left\{ {m \atop p} \right\}}{d-\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{d-\alpha} + \sum_{\alpha=p-1}^{d-1} p^s \cdot \binom{m}{\alpha} \cdot \binom{\left\{ {m \atop p} \right\}}{d-\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{d-\alpha} + \\ &+ p^{s-1} \cdot \left\{ {m \atop p} \right\} \left\{ {m \atop p-1} \right\} + p^{s-1} \cdot \sum_{\alpha=1}^{d-1} p^{s-1} \cdot \binom{\left\{ {m \atop p} \right\}}{\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{\alpha} \cdot \binom{d-1}{\alpha-1} \ \leq \ \operatorname{rank} m_v(x). \end{aligned} \tag{2.11}$$

$\square$

Proof. The proof immediately follows from cited upper results of [24] and from result (1.4) of Theorem 1.1.

Let's denote by

$$W(x) = \bigvee_{d} \left(\mathcal{F}^{p^{s-1}+1} \cdot H(x)^{p^{s-1}}\right).$$

Then according to (2.6) it is easy to see that

$$W(x) \mid m_v(x).$$

Further we shall investigate the form of polynomial $W(x)$. The polynomial $W(x)$ may be represented in this way:

$$\begin{aligned} &W(x) = \\ &= \operatorname*{LCM}_{\substack{(j_1,\dots,j_\alpha)\in\overline{0,m-1}^{\alpha},\ \alpha=\overline{0,d} \\ (\vec{\lambda}^{(1)},\dots,\vec{\lambda}^{(\beta)})\in\mathcal{I}(m,p)^{\beta}, \\ (\vec{\zeta}^{1)},\dots,\vec{\zeta}^{(\beta)})\in\mathcal{I}(m,p-1)^{\beta},\ \beta=d-\alpha}} \Bigg(x \ominus \theta_0^{p^{rj_1}+\dots+p^{rj_\alpha}} \cdot \\ &\cdot \theta_0^{\sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(1)}+p\zeta_l^{(1)})+\dots+\sum\limits_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l^{(\beta)}+p\zeta_l^{(\beta)})}\Bigg)^{\underbrace{p^{s-1}+1 \vee \dots \vee p^{s-1}+1}_{\alpha\ times} \vee \underbrace{p^{s-1} \vee \dots \vee p^{s-1}}_{d-\alpha\ times}} \end{aligned} \tag{2.12}$$

In (2.12) $\alpha = 0$ means that $\mathcal{F}$ is not consists in corresponding disjunctive product, and $\beta = 0$ means that $H(x)$ is not consists in corresponding disjunctive product.

Because

$$\begin{aligned} &\Bigg(\prod_{\alpha=1}^{p-2} \mathcal{F}^{(\alpha)}(x)^{(\alpha+1)p^{s-1}} \cdot \prod_{\alpha=p-1}^{d} \mathcal{F}^{(\alpha)}(x)^{p^s} \cdot \prod_{\alpha=1}^{p-2} W^{(\alpha)}(x)^{(\alpha+1)p^{s-1}} \cdot \\ &\prod_{\alpha=p-1}^{d-1} W^{(\alpha)}(x)^{p^s} \cdot \prod_{\alpha=1}^{d} H^{(\alpha)}(x)^{p^{s-1}}\Bigg) \Bigg| W(x), \end{aligned} \tag{2.13}$$

and

$$W(x) \mid m_v(x),$$

(2.10) holds. Inequality (2.11) follows from (2.10) and Lemma 2.4. □

Statement 2.6. In conditions of Theorem 2.5 these divisibilities hold:

$$p^{s-1} \mid \mathrm{T}(v) \mid (p^{rm}-1)p^s. \tag{2.14}$$

Besides that under additional condition

$$\mathrm{GCD}(d, p^{rm}-1) = 1 \tag{2.15}$$

this equality holds:

$$\mathrm{T}(m_v(x)) = (p^{rm}-1) \cdot p^s \tag{2.16}$$

$\square$

Proof. Let's remember that for every $\kappa \in \overline{1,d}$

$$\mathrm{T}(v^{(\kappa)}) = (p^{rm} - 1)p^s.$$

Hence

$$\mathrm{T}(v) \mid (p^{rm} - 1)p^s.$$

From the other side,

$$H(x) = \prod_{\substack{\vec{\lambda} \in \mathcal{I}(m,p), \\ \vec{\zeta} \in \mathcal{I}(m,p-1)}} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l + p\zeta_l)} \right),$$

and herewith

$$\vec{\lambda} = (0, \ldots, 0, 1, p-1) \text{ and } \vec{\zeta} = (0, \ldots, 0, p-1, 0)$$

$H^{(d)}(x)$ has a root of the form

$$\theta_0^{2rm} = e.$$

Hence

$$(x \ominus e)^{p^{s-1}} = x^{p^{s-1}} \ominus e \;\Big|\; m_v(x).$$

So divisibilities (2.14) are proved.

Further, polynomial $\mathcal{F}^{(d)}(x)$ has a root θ_0^d. Because under condition (2.15)

$$\operatorname{ord} \theta_0^d = \frac{(p^{rm} - 1)}{\mathrm{GCD}(p^{rm} - 1, d)} = p^{rm} - 1 \;\Bigg|\; \mathrm{T}(v),$$

and

$$\operatorname{ord} \theta_0^d = \operatorname{ord} \theta_0^{dp^s},$$

we get equalities:

$$(x \ominus \theta_0^d)^{p^s} = x^{p^s} \ominus \theta_0^{dp^s} \mid (x^{p^s})^{p^{rm}-1} \ominus e = x^{(p^{rm}-1)p^s} \ominus e.$$

So (2.16) holds. $\square$

3 Properties of design 1.13

In 1996 A.A.Nechaev had proved that if sequences $u_1, \ldots, u_m$ are obtained according to the rule (1.14) with matrix A of maximal period $\mathrm{T}(A) = (p^{rm} - 1)p^{n-1}$, then each of u_κ, $\kappa = \overline{1,m}$, is a MP LRS with Galois characteristic polynomial of maximal period $F(x) = \chi_A(x)$, which coincides with characteristic polynomial of matrix A. Moreover, in this case all LRS $u_1, \ldots, u_m$ are linearly independent over R. In [5] this result were published without referencing to A.A.Nechaev.

So we can apply results of previous section to the Design 1.13 herewith $m = d$.

Theorem 3.1. Let $R = GR(p^n, r)$ be a non-trivial Galois ring, $q = p^r$, $p \geq 5$, $r \geq 2$, $F(x)$ be a polynomial of maximal period and degree m over ring R, $u^{(1)}, \dots, u^{(m)}$ are non-zero modulo pR sequences with characteristic polynomial $F(x)$, satisfying the rule:

$$\left(u^{(1)}(i+1), \dots, u^{(m)}(i+1)\right) = A \cdot \left(u^{(1)}(i), \dots, u^{(m)}(i)\right), \ i \in \mathbb{N}_0, \tag{3.1}$$

$F(x) = \chi_A(x)$, $\mathrm{T}(A) = (p^{rm} - 1)p^{n-1}$, for $\kappa \in \overline{1, m}$ $w_\kappa = \gamma_s(u^{(\kappa)})$, $s \equiv 2 \pmod r$,

$$w = \prod_{\kappa=1}^{m} w_\kappa,$$

$S = GR(p^n, rm)$ be a Galois extension of R, θ be a root of $F(x)$ in S, polynomial $H(x)$ is defined as in (1.1), $\mathcal{F}(x) = \gamma_0(F(x))$.

Then

$$\begin{gathered}\Bigg(\prod_{\alpha=1}^{p-2} \mathcal{F}^{(\alpha)}(x)^{(\alpha+1)p^{s-1}} \cdot \prod_{\alpha=p-1}^{m} \mathcal{F}^{(\alpha)}(x)^{p^s} \cdot \prod_{\alpha=1}^{p-2} W^{(\alpha)}(x)^{(\alpha+1)p^{s-1}} \cdot \\ \prod_{\alpha=p-1}^{m-1} W^{(\alpha)}(x)^{p^s} \cdot \prod_{\alpha=1}^{m} H^{(\alpha)}(x)^{p^{s-1}}\Bigg) \ \Bigg| \ m_v(x)\end{gathered} \tag{3.2}$$

and

$$\begin{gathered} m + \sum_{\alpha=1}^{p-2} (\alpha+1)p^{s-1}\binom{m}{\alpha} \cdot \binom{m-1}{\alpha-1} + \sum_{\alpha=p-1}^{m-1} p^s \cdot \binom{m}{\alpha} \cdot \binom{m-1}{\alpha-1} + \\ + \sum_{\alpha=1}^{p-2} (\alpha+1)p^{s-1} \cdot \binom{m}{\alpha} \cdot \binom{\left\{ {m \atop p} \right\}}{m-\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{m-\alpha} + \sum_{\alpha=p-1}^{m-1} p^s \cdot \binom{m}{\alpha} \cdot \binom{\left\{ {m \atop p} \right\}}{m-\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{m-\alpha} + \\ + p^{s-1} \cdot \left\{ {m \atop p} \right\} \left\{ {m \atop p-1} \right\} + p^{s-1} \cdot \sum_{\alpha=1}^{m-1} p^{s-1} \cdot \binom{\left\{ {m \atop p} \right\}}{\alpha} \cdot \binom{\left\{ {m \atop p-1} \right\}}{\alpha} \cdot \binom{m-1}{\alpha-1} \ \leq \ \operatorname{rank} m_v(x). \end{gathered} \tag{3.3}$$

□

Statement 3.2. In conditions of Theorem 2.5 these divisibilities hold:

$$p^{s-1} \ \mid \mathrm{T}(w) \mid \ (p^{rm} - 1)p^s. \tag{3.4}$$

Besides that under additional condition

$$\mathrm{GCD}(m, p^{rm} - 1) = 1 \tag{3.5}$$

this equality holds:

$$\mathrm{T}(m_w(x)) = (p^{rm} - 1) \cdot p^s \tag{3.6}$$

□

References

[1] Bylkhov D. Second coordinate sequence of maximal period linear recurrence over ring $\mathbb{Z}_8$ // Problems of Discrete Mathematics. Addendum, 6, pp.9-10, (2013)

[2] M. A. Goltvanitsa, S. N. Zaitsev, A. A. Nechaev Skew linear recurring sequences of maximal period over galois rings // Journal of Mathematical Sciences, November 2012, Volume 187, Issue 2, pp 115–128

[3] Goresky, Mark; Klapper, Andrew // Algebraic shift register sequences, Cambridge: Cambridge University Press (ISBN 978-1-107-01499-2/hbk). xv, 498 p., 2012.

[4] Helleseth T., Martinsen M. Binary sequences of period $2^m - 1$ with large linear complexity // Informatrion and Computation, 151, 73–91, (1999)

[5] O.Khamlovsky Distribution properties of rows and columns of matrix linear recurrent sequences of first order Mathematical Issues of Cryptology, 6:4 (2015), 65–76

[6] Kurakin, V.L. Representations over $\mathbb{Z}_{p^n}$ of a linear recurring sequence of maximal period over $GF(p)$. (English; Russian original) Discrete Math. Appl. 3, No.3, 275-296 (1993); translation from Diskretn. Mat. 4, No.4, 96-116 (1992). Zbl 0811.11077

[7] Kurakin, V.L. The first coordinate sequence of a linear recurrence of maximal period over a Galois ring. (English; Russian original) Discrete Math. Appl. 4, No.2, 129-141 (1994); translation from Diskretn. Mat. 6, No.2, 88-100 (1994). Zbl 0824.11072

[8] Kurakin, V.L. The first digit carry function in the Galois ring. (English; Russian original) // Discrete Math. Appl. 22, No. 3, 241-259 (2012); translation from Diskretn. Mat. 24, No. 2, 21-36 (2012). Zbl 1281.11020

[9] Recovery of linear recurrence over primary residue ring from its complication Mathematical Issues of Cryptology, 1:2 (2010), 31–56 (In Russian)

[10] Kuzmin A.S., Nechaev A.A. Linear recurrent sequences over Galois rings // II Int.Conf.Dedic.Mem. A.L.Shirshov—Barnaul—Aug.20-25 1991 (Contemporary Math.—v.184—1995—p.237-254)

[11] Kuz'min A.S., Nechaev A.A. Linear recurring sequences over Galois rings. (Russian, English) // Algebra and Logic, Consultants Bureau (United States), vol. 34, num. 2, pp. 87-100 (1995)

[12] A.S.Kuzmin, A.A.Nechaev Reconstruction of MP LRS over Galois ring from its elder coordinate sequence, Discrete Mathematics and Applications, 2011, 21:2, 145–178

[13] Kurakin VL, Mikhalev AV, Nechaev AA, Tsypyschev VN Linear and polylinear recurring sequences over abelian groups and modules // Journal of Mathematical Sciences 102 (6), 4598-4626, 2000

[14] Nechaev, A.A. Kerdock code in a cyclic form. (English; Russian original) Discrete Math. Appl. 1, No.4, 365-384 (1991); translation from Diskretn. Mat. 1, No.4, 123-139 (1989). Zbl 0734.94023

[15] Nechaev, A.A. Linear recurrence sequences over commutative rings. (English; Russian original) Discrete Math. Appl. 2, No.6, 659-683 (1992); translation from Diskretn. Mat. 3, No.4, 105-127 (1991).Zbl 0787.13007

[16] Nechaev A.A. Cycle types of linear substitutions over finite commutative rings // Russian Academy of Sciences. Sbornik. Mathematics, vol. 78, num. 2, pp. 283-311 (1994)

[17] McDonald C. Finite rings with identity // New York: Marcel Dekker—1974—495p.

[18] Radghavendran R. A class of finite rings // Compositio Math.—1970— v.22—N1—p.49-57

[19] Sachkov, V.N. Introduction to combinatorial methods of discrete mathematics // Moscow, Nauka, 1982, 384P.

[20] Tsypyschev V.N. Matrix linear congruent generator over a Galois ring of odd characteristic // Proceedings of the 5th Int. Conf. "Algebra and number theory: modern problems and applications", Tula State Pedagogic Univ., Tula, 2003, p 233-237 (In Russian) MathSciNet: 2035586

[21] Tsypyschev, V.N. Rank estimations of the second coordinate sequence of MP-LRS over nontrivial Galois ring of odd characteristic (in Russian) // II Int. Sci. Conference on Problems of Security and Counter-Terrorism Activity — Moscow, MSU, October 25-26, 2006 — Proceedings published by Moscow Independent Center for Mathematical Education—2007—pp287–289

[22] Tsypyschev, V.N. Second coordinate sequence of the MP-LRS over nontrivial Galois ring of odd characteristic // IV International Symposium "Current Trends in Cryptology"CtCrypt'2015, June,3–5,2015, Kazan, Proceedings. Available at IACR e-print Archive, http://eprint.iacr.org/2015/1040

[23] V.N.Tsypyschev Low Linear Complexity Estimates for Coordinate Sequences of Linear Recurrences of Maximal Period over Galois Ring // http://eprint.iacr.org/2016/212

[24] N.Zierler, W.Mills Products of linear recurring sequences // J. of Algebra—27(1973)—pp.147-157