Second coordinate sequence of the MP-LRS over non-trivial Galois ring of the odd characteristic

Vadim N.TSYPYSCHEV [*]

Abstract

We investigate a well-known way to construct pseudo-random sequences by separation p-adic coordinate sequences of linear recurrences over Galois ring. Commonly it is necessary to know rank estimations of separated sequences.

In this article we describe divisors of the minimal polynomial of the second p-adic coordinate sequence of the linear recurrent sequence of maximal period/MP-LRS over non-trivial Galois ring of odd characteristic in dependence of the initial vector of this LRS.

Also we describe polynomials divisible by that minimal polynomial in dependence of the initial vector of this LRS.

As a corollary we get non-trivial upper and lower estimations for the rank of the second coordinate sequence of such MP-LRS which provides us by possibility to use it in pseudo-random generation.

We say that the Galois ring is *non-trivial*, if it differs from Galois field and from quotient ring too.

These results were worked out with participation of V.L.Kurakin as a supervisor. Author is very grateful to V.L.Kurakin for his participation in this work

Keywords: linear recurrent sequence, minimal polynomial, rank estimations, pseudo-random sequences.

1 Introduction

Let $R = GR(p^n, r)$ be a Galois ring [11, 12], $q = p^r$, p is a prime, u is a linear recurrent sequence of the full period over R with characteristic Galois polynomial $F(x)$ of degree m [7].

[*] This report is dedicated to the memory of Prof.A.A.Nechaev and Dr.V.L.Kurakin

Let $S = GR(p^n, rm)$, $Q = q^m$, be a Galois extension of R, splitting ring of the polynomial $F(x)$, θ is a root of $F(x)$ in the ring S. Then [6] there exists an unique constant $\xi \in S$ with property :

$$u(i) = \mathrm{Tr}_R^S(\xi\theta^i), \ i \in \mathbb{N}_0, \tag{1}$$

where $\mathrm{Tr}_R^S(x) = \sum\limits_{\sigma \in \mathrm{Aut}(S/R)} x^\sigma$ is a *trace* function from the ring S into ring R.

It is known that the arbitrary element $s \in S$ may be uniquely represented in the form

$$s = \sum_{i=0}^{n-1} \gamma_i(s)p^i, \ \gamma_i(s) \in \Gamma(S), \ i = \overline{0, n-1}, \tag{2}$$

where $\Gamma(S) = \{x \in S \mid x^Q = x\}$ is a *p-adic coordinate set of the ring S (Teichmueller's representatives system).*

The set $\Gamma(S)$ with operations $\oplus : x \oplus y = (x+y)^{Q^n}$ and $\otimes :\ x \otimes y = xy$ is a Galois field $GF(Q)$.

The field $\Gamma(S)$ contains as a sub field the set $\Gamma(R) = \{x \in R \mid x^q = x\}$ which is a p-adic coordinate set of the ring R.

Operations on elements of the $\Gamma(R)$ are defined in the same way. Because of that the set $\Gamma(R)$ is a field $GF(q)$.

It is known that [11, 12] the group $\mathrm{Aut}(S/R)$ is a cyclic and is generated by the *Frobenius automorphism* ρ which acts upon the element $s \in S$ of the form (2) according to the rule

$$\rho(s) = \sum_{i=0}^{n-1} \gamma_i(s)^q p^i. \tag{3}$$

Representation analogous to the (2) takes place for elements of the ring R.

The sequence $u(i)$, $i \in \mathbb{N}_0$, uniquely determines n *p-adic coordinate sequences* $u_l(i) = \gamma_l(u(i))$, $l = \overline{0, n-1}$, $i \in \mathbb{N}_0$, over the field $(\Gamma(R), \oplus, \cdot)$.

If we have a task to generate a pseudo random sequences relying on linear recurrence over Galois ring we may choose one or several elder coordinate sequences of this linear recurrence. In this way it is interesting to have estimations for the ranks of those coordinate sequences $\gamma_l(u)$, $l = \overline{0, n-1}$.

In the work [10] were obtained lower and upper estimations for the ranks of coordinate sequences of linear recurrences of maximal period over primarily residue rings. Besides that, there were obtained minimal polynomials of coordinate sequences for some types of such linear recurrences.

Also in the work [10] were obtained minimal polynomials of sequences u_l, $l = \overline{0,1}$, over nontrivial Galois ring.

In the article [3] were obtained the minimal polynomial and the rank of the first coordinate sequence of linear recurrence u over non-trivial Galois ring determined in arbitrary coordinate set.

Further in the article [9] were obtained exact values of ranks for second coordinate sequence of faithful linear recurrent sequence over binary residue ring with minimal Galois polynomial of degree not less then 5 in dependence on the initial vector of this LRS.

Below we will provide polynomials over Galois field $\Gamma(R)$ which respectively divides and are divisible by minimal polynomial of the second coordinate sequence of the linear recurrence u in p-adic coordinate set under condition of $p \geq 5$. These results provide a way to obtain upper and lower estimations for the rank of this linear recurrence. Previously these results in less faithful form were published in [15].

Furthermore, relying on these results in the next article we will obtain rank estimations for elders coordinate sequences of MP LRS over nontrivial Galois ring with specially selected numbers.

2 Main results

Let $M, w \in \mathbb{N}$. We will denote by $\mathcal{I}(M,w)$ the set of strings $\vec{\jmath} = (j_1, \ldots, j_M)$, $0 \leq j_l \leq p-1$, $l = \overline{1,M}$, with property : $\sum_{l=1}^{M} j_l = w$.

By $\left\{ {M \atop w} \right\}$ we will denote the cardinality of the set $\mathcal{I}(M,w)$. Let us note that $\left\{ {M \atop w} \right\}$ is equal to the quantity of allocations of w identical balls into M different boxes under condition that into each box there disposes not greater then $p-1$ balls. It is known that [8, C.215]:

$$\left\{ {M \atop w} \right\} = \sum_{s=0}^{\min\{w,(M-w)/p\}} (-1)^s \binom{w}{s} \binom{M+w-ps-1}{M-1}, \qquad (4)$$

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

$$\left\{ \begin{matrix} M \\ w \end{matrix} \right\} = 0 \qquad (5)$$

in other case.

Let m is a degree of some polynomial under investigation. Further we will denote by $N = N(m)$ the value $\left\{ \begin{smallmatrix} m \\ p \end{smallmatrix} \right\}$. Besides that, we will concern that the strings $\vec{\jmath}^{(1)}, \ldots, \vec{\jmath}^{(N)}$ in the set $\mathcal{I}(m,p)$ are allocated in the lexicographical order.

Let $R = GR(p^n, r)$ be a Galois ring, $q = p^r$, $p \geq 5$, $r \geq 2$, $F(x)$ is a Galois polynomial of degree m over the ring R, the sequence $u \in L_R(F)$ is a non-zero by modulus pR and is represented by the trace-function

$$u(i) = \mathrm{Tr}_R^S(\xi\theta^i),$$

where $S = GR(p^n, rm)$ is a splitting ring of the polynomial $F(x)$, θ is a root of $F(x)$ in the S, the constant $\xi \in S$ is unequally determined . Let , further, $Q = q^m = p^t$, $t = rm$, $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$.

The element ∇ is introduced in this way: according to Wilson theorem we have $(p-1)! \underset{p}{\equiv} -1$. Hence when $p \geq 3$ number $(p-1)!$ as an element of the ring $\mathbb{Z}_{p^n}$ has a p-adic representation of the form

$$(p-1)! \underset{p^2}{\equiv} -1 - p\nabla, \nabla \in \Gamma(\mathbb{Z}_{p^n}).$$

Let's denote:

$$G(x) = \prod_{\vec{\jmath} \in \Xi} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} j_l p^{rm+rl-1}} \right),$$

$$\Xi = \left\{ \vec{\jmath} \in \mathcal{I}(m,p) : \nabla \cdot \gamma_0 \left(\frac{1}{\prod_{l=0}^{m-1} j_l!} \right) \neq \ominus \gamma_1 \left(\frac{1}{\prod_{l=0}^{m-1} j_l!} \right) \right\},$$

$$W(x) = \prod_{s=0}^{p} \prod_{(\vec{\lambda}, \vec{\zeta}) \in \Omega_s} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{t+rl-2}(\lambda_l + p\zeta_l)} \right),$$

where

$$\Omega_s = \left\{ (\vec{\lambda}, \vec{\zeta}) \;:\; \vec{\lambda} \in \mathcal{I}(m, ps), \vec{\zeta} \in \mathcal{I}(m, p-s), \right.$$
$$\left. \sum_{\substack{\vec{\mu} \in \mathcal{I}(N,p): \\ \sum_{i=1}^{N} \mu_i \cdot j_l^{(i)} = \lambda_l + p\zeta_l, l = \overline{0, m-1}}} \!\!\!\!\!\bigoplus \gamma_0 \left(\frac{1}{\prod_{i=1}^{N} \mu_i! (\prod_{l=0}^{m-1} j_l^{(i)}!)^{\mu_i}} \right) \neq 0 \right\}, s = \overline{0, p},$$

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

$$H(x) = H_1(x), Z(x) = H_0(x),$$

$$D_1(x) = \text{ GCD } (G(x), W(x)),\ D_2(x) = \text{GCD } (W(x), H(x)).$$

Pay attention to the fact

$$G(x) \mid Z(x).$$

Besides that, let's denote by

$$\tilde{F}(x) = \gamma_0(F(x))$$

the polynomial obtained from $F(x)$ by picking out zeroth p-adic digits of every coefficient of polynomial. It is obviously that $\tilde{F}(x) \in \bar{F}(x)$, where $\bar{F}(x)$ is a residue class of the $F(x)$ in the ring $R[x]/pR[x]$.

Theorem 2.1 *Let $R = GR(p^n, r)$ be a Galois ring, $q = p^r$, $p \geq 5$, $r \geq 2$, $F(x)$ is a Galois polynomial of degree m over the ring R, the sequence $u \in L_R(F)$ is a non-zero by modulus pR and is represented by the trace-function*

$$u(i) = \mathrm{Tr}_R^S(\xi\theta^i),$$

where $S = GR(p^n, rm)$ is a splitting ring of the polynomial $F(x)$, θ is a root of $F(x)$ in the S, the constant $\xi \in S$ is unequally determined . Let , further, $Q = q^m = p^t$, $t = rm$, $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$.

If $F(x)$ is a MP-polynomial, in other words [14], θ_0 is a primitive element of the field $\Gamma(S) = GF(Q)$, and $\theta_1 \neq 0$, then for a minimal polynomial of the second coordinate sequence u_2 of the LRS u in the p-adic coordinate set these dependencies hold:

$$\tilde{F}(x)^{p+1} \cdot \frac{G(x)}{D_1(X)} \cdot \frac{W(x)}{D_1(x) \cdot D_2(x)} \cdot H(x)^p \;\Bigg|\; m_2(x),$$

$$m_2(x) \;\Bigg|\; \tilde{F}(x)^{p+1} \cdot Z(x)^{\epsilon} \cdot H(x)^p \cdot \text{ LCM } \left(\frac{W(x)}{D_2(x)}, \prod_{s=2}^{p-1} H_s(x)^{\beta_s}\right).$$

Under the same conditions these inequalities hold:

$$\epsilon \le p, \quad \beta_s \le p-1, s = \overline{2, p-1}.$$

Besides that in described cases there known equal values of the parameter ϵ*:*

(a) If $\xi_1 \neq 0$*, then under additional conditions*

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

and

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

the equality holds: $\epsilon = p$*, and* $Z(x)^\epsilon \mid m_2(x)$*.*

(b) If $\xi_1 = 0$*, then* $\epsilon = 2$*.*

Under the same condition

$$Z(x)^\epsilon \mid m_2(x).$$

Let's note that this time neither equal value of the parameter $\deg G(x)$ nor its upper bound are not obtained.

It is clear that this parameter is not greater then

$$\left\{ \begin{matrix} m \\ p \end{matrix} \right\},$$

and also depends on p.

Something the same may be declared about parameters $\deg W(x)$ and $\deg D_i(x), i = \overline{1,2}$.

The same reasoning as in proof of the Theorem 2.1 is valid in the case of $R = \mathbb{Z}_{p^n}$.

However under condition $r = 1$ all previous symbolization becomes invalid and because of that all previous rank estimations become invalid too.

Theorem 2.2 *I. Under conditions of the Theorem 2.1 these inequalities hold:*

$$\begin{aligned} m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} \leq \operatorname{rank} u_2 \leq\ & m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} + \\ & +(p-1)\sum_{s=2}^{p-1}\left\{ {m \atop ps} \right\}\left\{ {m \atop p-s} \right\} + \\ & +p\left\{ {m \atop p} \right\} + \left\{ {m \atop p^2} \right\}. \end{aligned}$$

II. Moreover, under additional conditions these inequalities hold:

(a) If $\xi_1 \neq 0$,

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

and

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

then:

$$\begin{aligned} m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} + p\left\{ {m \atop p} \right\} \leq \operatorname{rank} u_2 \leq\ & m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} + \\ & +(p-1)\sum_{s=2}^{p-1}\left\{ {m \atop ps} \right\}\left\{ {m \atop p-s} \right\} + \\ & +p\left\{ {m \atop p} \right\} + \left\{ {m \atop p^2} \right\}. \end{aligned}$$

(b) If $\xi_1 = 0$, then:

$$\begin{aligned} m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} + 2\left\{ {m \atop p} \right\} \leq \operatorname{rank} u_2 \leq\ & m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} + \\ & +(p-1)\sum_{s=2}^{p-1}\left\{ {m \atop ps} \right\}\left\{ {m \atop p-s} \right\} + \\ & +2\left\{ {m \atop p} \right\} + \left\{ {m \atop p^2} \right\}. \end{aligned}$$

References

[1] Elwyn R.Berlekamp Algebraic Coding Theory (English) // Zbl 0988.94521 New York, NY: McGraw-Hill Book. xiv, 466 p. (1968).

[2] 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

[3] 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

[4] 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

[5] Lidl, Rudolf; Niederreiter, Harald Finite fields. // 2nd edition— 1996 (English) — Encyclopedia of Mathematics and Its Applications— 20— Cambridge: Cambridge University Press (ISBN 978-0-521-06567-2/pbk)— 755 p. — Zbl 1139.11053

[6] 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

[7] 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

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

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

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

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

[13] V. N. Tsypyshev 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

[14] Tsypyschev, V.N. Full periodicity of Galois polynomials over nontrivial Galois rings of odd characteristic. (English. Russian original) Zbl 1195.11160 // J. Math. Sci., New York 131, No. 6, 6120-6132 (2005); translation from Sovrem. Mat. Prilozh. 2004, No. 14, 108-120 (2004)

[15] Tsypyschev, V.N. Rank estimations of the second coordinate sequance 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

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