Low Linear Complexity Estimates for Coordinate Sequences of Linear Recurrences of Maximal Period over Galois Ring

Abstract

In this work we provide low rank estimations for 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 $s = kr + 2$, $k \in \mathbb{N}_0$.

Keywords: linear recurrent sequence, linear complexity/rank estimations, pseudo-random sequences.

1 Introduction

Pseudo-random sequences are essential ingredients of every modern digital communication system including cellular telephones, GPS, secure internet transactions and satellite imagery. Each application requires pseudo-random sequences with specific properties. This article describes the design and properties of pseudo-random sequences, obtained from those generated strictly by shift registers over Galois rings.

Let $R = GR(p^n, r)$ be a Galois ring [12, 13], $q = p^r$, 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 [10].

Let $\mathrm{T}(F)$ denote a period of polynomial $F(x)$, i.e. minimal t with property: $F(x) \mid x^{\lambda}(x^t - e)$ for some $\lambda \geq 0$.

Let $\bar{F}(x)$ be an image of $F(x)$ under canonical epimorphism $R[x] \to R[x]/pR[x]$.

Let remind [11], that :

$$\mathrm{T}(\bar{F}(x)) \,|\mathrm{T}(F(x))|\, \mathrm{T}(\bar{F}(x)) \cdot p^{n-1}.$$

Polynomial $F(x)$ is called distinguished , if

$$\mathrm{T}(F) = \mathrm{T}(\bar{F}),$$

and is called polynomial of full period , if

$$\mathrm{T}(F) = \mathrm{T}(\bar{F}) \cdot p^{n-1}.$$

Under additional condition $\mathrm{T}(\bar{F}) = q^m - 1$, polynomial $F(x)$ is called polynomial of maximal period (MP-polynomial) . Unitary and reversible polynomial we call regular.

Galois ring $R = GR(p^n, r)$ is called nontrivial iff $n > 1$, $r \geq 2$, i.e. iff R is neither field nor residue ring of integers .

It is well-known [1] that for the synthesis of algebraic shift registers over finite fields, rings or modules in most cases are necessary to construct polynomials with high periodic properties.

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 [9] there exists an unique constant $\xi \in S$ with property :

$$u(i) = \mathrm{Tr}_R^S(\xi\theta^i),\ i \in \mathbb{N}_0, \tag{1.1}$$

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

$$s = \sum_{i=0}^{n-1} \gamma_i(s) p^i,\ \gamma_i(s) \in \Gamma(S),\ i = \overline{0, n-1}, \tag{1.2}$$

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 $\oplus : x \oplus y = (x + y)^{Q^{n-1}}$ 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 [12, 13] 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 (1.2) according to the rule

$$\rho(s) = \sum_{i=0}^{n-1} \gamma_i(s)^q p^i. \tag{1.3}$$

Representation analogous to the (1.2) 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 $(\Gamma(R), \oplus, \cdot)$.

Herewith if u is a linear recurrence of maximal period $\mathrm{T}(u) = (p^{rm} - 1)p^{n-1}$, then for every $s \in \overline{0, n-1}$ $\mathrm{T}(u_s) = (p^{rm} - 1)p^{s-1}$, i.e. u_s also has large period.

Let us denote by $m_s(x)$ the minimal polynomial of the sequence u_s, $s = \overline{0, n-1}$, over the field $\Gamma(R)$. By the linear complexity or rank of the sequence u_s we denote the degree of its minimal polynomial: $\mathrm{rank} u_s = \deg m_s(x)$.

If we have a task to generate a pseudo-random sequence relying on linear recurrence over Galois ring we may choose one or several elder coordinate sequences of this linear recurrence:

$$u(i) \quad \mapsto \quad \begin{matrix} u_{n-1}(i) = \gamma_{n-1}\left(u(i)\right) \\ \vdots \\ u_0(i) = \gamma_0\left(u(i)\right) \end{matrix} \quad \mapsto \quad u_s(i) = \gamma_s\left(u(i)\right). \tag{1.4}$$

In this case it is important to have estimations for the linear complexity/ranks of those coordinate sequences $\gamma_l(u)$, $l = \overline{0, n-1}$, because it is well-known that the linear complexity is a parameter which characterizes the power of pseudo-random sequence in relation to linearization method of cryptanalysis.

In the work [6] 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 [6] were obtained minimal polynomials of sequences u_l, $l = \overline{0, 1}$, over nontrivial Galois ring.

In the article [4] 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 [2] 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.

In [16] were provided 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 the second coordinate sequence of this linear recurrence.

In this article we follow-up the pevious work [16] and obtain lower estimations for linear complexity of coordinate sequences u_s of LRS MP under condition $s \equiv 2 \pmod{r}$, $p \geq 5$, where $R = GR(p^n, r)$.

Let $M, w \in \mathbb{N}$. Let's denote by $\mathcal{I}(M, w)$ the set of vectors $\vec{\jmath} = (j_1, \ldots, j_M)$, $0 \leq j_l \leq p-1$, $l = \overline{1, M}$, 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 [14, p.215]:

$$\left\{ {M \atop w} \right\} = \sum_{s=0}^{\min\{w, (M-w)/p\}} (-1)^s \binom{w}{s} \binom{M + w - ps - 1}{M - 1}, \tag{1.5}$$

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

$$\left\{ \begin{matrix} M \\ w \end{matrix} \right\} = 0 \tag{1.6}$$

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 u be a linear recurrent sequence of maximal period over ring R [10] with minimal polynomial $F(x)$. Let's denote by $\mathcal{F}(x) = \gamma_0(F(x))$. It is known that [6]

$$\mathcal{F}(x)^{p^{s-1}+1} \,\Big|\, m_s(x), \;\; s = \overline{1, n-1},$$

where by the estimate of Nechaev–Kuzmin follows:

$$m(p^{s-1}+1) \le \operatorname{rank} u_s, \;\; s \ge 0. \tag{1.7}$$

Let $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$.

If $F(x)$ is a polynomial of maximal period then θ_0 is a primitive element of the field $\Gamma(S)$ and $\theta_1 \ne 0$.

Let

$$H(x) = \prod_{\substack{\vec{\lambda} \in \mathcal{I}(m,p),\\ \vec{\zeta} \in \mathcal{I}(m,p-1)}} \left(x \ominus \theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l + p\zeta_l)} \right), \tag{1.8}$$

where $\vec{\lambda} = (\lambda_0, \ldots, \lambda_{m-1})$, $\vec{\zeta} = (\zeta_0, \ldots, \zeta_{m-1})$.

It is known [16, Theorem 2.1] that if u is a linear recurrent sequence (LRS) of maximal period (MP) over non-trivial Galois ring then

$$H(x)^p \mid m_2(x). \tag{1.9}$$

Moreover, [16, Theorem 2.1] if $\xi_1 \ne 0$ and additional conditions fulfill:

$$\forall \vec{\zeta} \in \mathcal{I}(m,p) \quad \sum_{\kappa = \overline{0,m-1} \,:\, \zeta_\kappa > 0}^{\oplus} (\xi_0^{-1}\xi_1)^{p^{rm+r\kappa-1}} \ne 0 \tag{1.10}$$

and

$$\forall \vec{\zeta} \in \mathcal{I}(m,p) \quad \sum_{l = \overline{0,m-1} \,:\, \zeta_l > 0}^{\oplus} \gamma_0 \left(\frac{\zeta_l}{\prod_{\kappa=0}^{m-1} \zeta_\kappa !} \right) (\theta_0^{-1}\theta_1)^{\sum_{\kappa=0}^{m-1} \zeta_\kappa p^{rm+r\kappa-1} - p^{rm+rl-1}} \ne 0, \tag{1.11}$$

then for polynomial

$$Z(x) = \prod_{\vec{\zeta} \in \mathcal{I}(m,p)} \left(x \ominus \theta_0^{\sum\limits_{l=0}^{m-1} p^{rm+rl-1} \cdot \zeta_l} \right) \tag{1.12}$$

this relation fulfills:

$$Z(x)^p \ \mid m_2(x)\ . \tag{1.13}$$

Let u be a LRS MP over ring $R = GR(p^n, r)$ with minimal polynomial $F(x)$. In [6, Теорема 1.3] were proved that for arbitrary Galois ring $R = GR(p^n, r)$, $q = p^r$, and for arbitrary $s \in \overline{1, n-1}$ equalities accomplish:

$$m_s(x) = \mathcal{F}(x)^{p^{s-1}+1} \cdot f_{s,1}(x)^{p^{s-1}} \cdots f_{s,k}(x)^{p^{s-1}-k+1} \cdots f_{s,p^{s-1}}(x), \tag{1.14}$$

where $f_{s,k}(x)$ is separable polynomial, $k = \overline{1, p^{s-1}}$, and

$$\mathcal{F}(x) \cdot f_{s,1}(x) \cdots f_{s,p^{s-1}}(x) \mid x^{\tau_0} \ominus e, \tag{1.15}$$

where

$$\tau_s = (q^m - 1)p^s,\ m = \deg F(x),\ s = \overline{0, n-1}.$$

Because $F(x)$ is a polynomial of maximal period for $s = \overline{0, n-1}$ this equality holds:

$$x^{\tau_s} - e \equiv p^{s+1}\Phi_{s+1}(x) \pmod{F(x)}, \tag{1.16}$$

herewith

$$\deg \Phi_{s+1}(x) < m,\ \bar{\Phi}_{s+1}(x) \neq 0.$$

Following the article [4] let's denote

$$u^{(s)} = \Phi_s(x) \cdot u,\ \text{and}\ u_t^{(s)} = \gamma_t(u^{(s)}),\ s, t = \overline{0, n-1}. \tag{1.17}$$

If $p \geq 3$ for arbitrary Galois ring R it is proved [6, Лемма 2.1]:

$$u_0^{(s)} = u_0^{(1)}, s \geq 1,\ \text{и}\ u_1^{(s)} = u_1^{(2)}, s \geq 2. \tag{1.18}$$

Besides that if by $u_{s,t}$ denoted sequence of form

$$u_{s,t} = (x^{\tau_0} \ominus e)^{p^{s-1}-p^t} \cdot u_s,\ s \geq t+2, t \geq 0, s, t \in \overline{0, n-1}, \tag{1.19}$$

then this state takes place:

Statement 1.1 (Dorofeev N.V., 1993, personal communication). In the case of non-trivial Galois ring $R = GR(p^n, r)$, $q = p^r$, $r \geq 2$, $p \geq 3$, these relations hold:

$$u_{s,s-2}^p = (u_0^{(1)})^{(p-1)p^r} \cdot u_{s-1} \ominus \frac{(u_0^{(1)})^p}{2} \oplus \xi(p, s, t), \tag{1.20}$$

and for $t < s - 2$

$$u_{s,t}^{p^{s-t-1}} = (u_0^{(1)})^{(p-1)\sum_{i=0}^{s-t-2} p^{r+i}} \cdot u_{t+1} \ominus \frac{(u_0^{(1)})^{p+(p-1)\sum_{i=1}^{s-t-2} p^{r+i}}}{2} \oplus \xi(p, s, t), \tag{1.21}$$

where

$$\xi(p, s, t) = \begin{cases} \left(\bar{\Phi}_1(x)^2 \cdot u_0\right)^p, & p = 3, t = 0, s = 2, \\ \left(\bar{\Phi}_1(x)^2 \cdot u_0\right)^p \cdot (u_0^{(1)})^{(p-1)\sum_{i=1}^{s-2} p^{r+i}}, & p = 3, t = 0, s > 2, \\ 0, & \text{in other cases} \end{cases} \tag{1.22}$$

□

Let's note that in [7, (2.13)] A.S.Kuzmin has published previously obtained analogous results for the case of $\mathbb{Z}_{p^n}$.

2 Main result

Theorem 2.1. 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 (1.1).

Let $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$,

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

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

Then for every natural $s > 2$ such that

$$s \equiv 2 \pmod{r}, \tag{2.1}$$

this inequality holds:

$$m(p^{s-1}+1) + p^{s-1} \cdot \begin{Bmatrix} m \\ p \end{Bmatrix} \cdot \begin{Bmatrix} m \\ p-1 \end{Bmatrix} \leq \operatorname{rank} u_s. \tag{2.2}$$

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

$$\forall\vec{\zeta} \in \mathcal{I}(m,p) \quad \sum_{\kappa=\overline{0,m-1}\ :\ \zeta_\kappa>0}\!\!\oplus \quad (\xi_0^{-1}\xi_1)^{p^{rm+r\kappa-1}} \neq 0 \tag{2.3}$$

and

$$\forall\vec{\zeta} \in \mathcal{I}(m,p) \quad \sum_{l=\overline{0,m-1}\ :\ \zeta_l>0}\!\!\oplus \quad \gamma_0\left(\frac{\zeta_l}{\prod_{\kappa=0}^{m-1}\zeta_\kappa!}\right)(\theta_0^{-1}\theta_1)^{\sum_{\kappa=0}^{m-1}\zeta_\kappa p^{rm+r\kappa-1} - p^{rm+rl-1}} \neq 0, \tag{2.4}$$

then for those s inequality takes place:

$$m(p^{s-1}+1) + p^{s-1} \cdot \begin{Bmatrix} m \\ p \end{Bmatrix} \cdot \begin{Bmatrix} m \\ p-1 \end{Bmatrix} + p^{s-1} \cdot \begin{Bmatrix} m \\ p \end{Bmatrix} \leq \operatorname{rank} u_s. \tag{2.5}$$

□

Proof. Let $s \geq 3$. Then according to (1.21), (1.22),

$$\begin{cases} u_{s,0}^{p^{s-1}} = (u_0^{(1)})^{p^{s-1}-1} \cdot u_1 \ominus \frac{(u_0^{(1)})^{p^{s-1}}}{2}, \\ u_{2,0}^{p} = (u_0^{(1)})^{p-1} \cdot u_1 \ominus \frac{(u_0^{(1)})^{p}}{2}. \end{cases} \tag{2.6}$$

Let's note that in those tact $i \in \mathbb{N}_0$ when $u_0^{(1)}(i) = 0$ also

$$u_{2,0}(i) = u_{s,0}(i) = 0. \tag{2.7}$$

Therefor further we concern only those tact $i \in \mathbb{N}_0$ when $u_0^{(1)}(i) \neq 0$.

From (2.6), and previous equations, and conditions of the Theorem follow that if

$$s \equiv 2 \pmod r, \tag{2.8}$$

then that system of equalities will take a form:

$$\begin{cases} u_{s,0}^{p} = (u_0^{(1)})^{p-1} \cdot u_1 \ominus \frac{(u_0^{(1)})^{p}}{2}, \\ u_{2,0}^{p} = (u_0^{(1)})^{p-1} \cdot u_1 \ominus \frac{(u_0^{(1)})^{p}}{2}. \end{cases} \tag{2.9}$$

Indeed if $s - 2 = kr$, $k \in \mathbb{N}$, then

$$p^r - 1 \,\Big|\, p^{kr} - 1 = p^{s-2} - 1.$$

and

$$p^r - 1 \,\Big|\, p\left(p^{s-2} - 1\right) = \left(p^{s-1} - 1\right) - (p-1),$$

where from for arbitrary $\alpha \in \Gamma(R) \setminus \{0\}$

$$\alpha^{\left(p^{s-1}-1\right)-(p-1)} = e$$

or

$$\alpha^{p^{s-1}-1} = \alpha^{p-1}.$$

Hence under condition (2.8) the equality takes place:

$$u_{s,0} = u_{2,0}. \tag{2.10}$$

This way under condition (2.8),

$$m_{u_{s,0}}(x) = m_{u_{2,0}}(x). \tag{2.11}$$

Because for arbitrary Galois ring this equality holds:

$$m_{u_{s,t}}(x) = \frac{m_{u_s}(x)}{\text{НОД}\left(m_{u_s}(x), (x^{\tau_0} \ominus e)^{p^{s-1}-p^t}\right)} = \mathcal{F}(x)^{p^t+1} \cdot f_{s,1}^{p^t} \cdots f_{s,p^t}(x), \tag{2.12}$$

hence for $p \geq 5$ this equality takes place:

$$f_{s,1}(x) = f_{2,1}(x). \tag{2.13}$$

Since

$$H(x) \mid f_{2,1}(x), \tag{2.14}$$

then from here with considering equality (1.14) inequality (2.2) follows.

Besides that, taking into account conditions $\xi_1 \neq 0$, (2.3), (2.4) we can deduce that this relation holds:

$$Z(x) \mid f_{2,1}(x) \ , \tag{2.15}$$

from which it follows relation (2.5). □

3 Conclusions

It is easy to see that estimations (2.2), (2.5) largely improve previously known Kuzmin–Nechaev estimation (1.7), [6].

Weakness of newly acquired estimates consists in that the new estimates extends not at all coordinate sequences u_s, $s = \overline{0, n-1}$.

From the other side for the case $r = 1$, $p \geq 3$, i.e. $R = \mathbb{Z}_{p^n}$, in [7, (1.24)] were obtained estimate

$$\operatorname{rank} u_s \geq m(p^{s-1} + 1) + \left\{ \begin{matrix} m \\ p^s \end{matrix} \right\}, \ s = \overline{0, n-1}.$$

It shows a deep difference between cases of non-trivial Galois ring and residue ring of integers.

References

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

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

[3] 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

[4] 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

[5] 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

[6] 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)

[7] 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)

[8] 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

[9] 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

[10] 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

[11] 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)

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

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

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

[15] 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

[16] 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, 2015, 1040