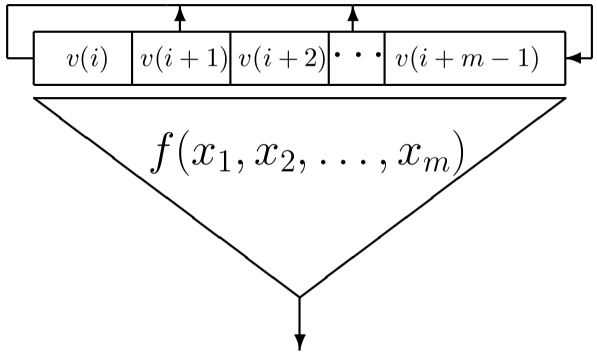
Oleg Kozlitin

Pseudo-random generators based on shift registers over finite commutative rings

Introduction

One of the most popular ways of pseudo-random sequence constructing is to use the shift registers over finite commutative rings. The shift register with linear feedback function (LFSR) and non-linear output function is a classical representative of such kind generators. There are a lot of cryptographic parameters of LFSR which have to be studied. Among them are the periodical properties, the statistical properties and the linear complexity (rank) of output sequence. Consideration of these parameters is a main content of many papers. In that connection, mention must be made of the articles by A.A. Nechaev, V.L. Kurakin, A.S. Kuzmin, A.V. Mikhalev, V.N. Tsypyshev, O.V. Kamlovskiy, D.N. Bylkov and other authors.



The aim of this report is to describe two methods of generalization of the classical LFSR. The first method is to use polynomial feedback function. The pseudo-random generator with polynomial feedback function is called polynomial generator. The polynomial shift register is a special case of the polynomial generator. The polynomial generator over residue ring was investigated in the articles by V.S. Anashin and M.V. Larin. Some results about periodical properties of polynomial generator over arbitrary finite commutative ring with identity were received by V.E. Viktorenkov. The cycle structure of polynomial generator over Galois ring was described by D.M. Ermilov.

In this report the periodical properties of polynomial generator over finite chain ring (finite commutative local ring of main ideals) and the cycle structure of multidimensional polynomial generator over Galois ring will be discussed.

The second method of generalization is to use several linear feedback functions instead of one linear feedback function. The use of multidimensional linear shift register (k-LFSR) is one of the possible ways to solve this problem. Originally, k-LFSR was proposed by Japanese mathematicians T. Nomura and A. Fukuda as a decoder of two-dimensional cyclic code. Later this automation was studied by A.A. Nechaev, A.V. Mikhalev, V.L. Kurakin and A.S. Kuzmin as a pseudo-random generator. Since 2003, the so-called self-controlled k-LFSR has been investigated. Some cryptographic properties of output sequence of self-controlled 2-LFSR over Galois ring will be described in this report. Also we will discuss the ways of optimal choice of the automation's parameters (an output function and a control function).

Polynomial generator

Let's discuss the multidimensional (m-dimensional) polynomial generator over ring R and list the main results concerning this issue. Let R be a finite chain ring. Under the condition $m = 1$, the upper limit of the length of the maximum cycle in the polynomial transformation graph is found. For arbitrary m and for Galois ring R the maximum length $L_m(R)$ of cycles of bijective polynomial transformations is calculated. A polynomial transformation having a cycle of length $L_m(R)$ is called transformation with a cycle of maximum length (CML-transformation). The work presented by this report describes CML-transformations. An algorithm for constructing CML-transformations is proposed. In some special cases, the cyclic structure of CML-transformation is described.

Let's describe the results in more detail. Consider $f(x) \in R[x]$. The *polynomial generator* over ring R generates a sequence $u \in R^\infty$ of the following form:

$$\forall\, i \geq 0 : \quad u(i+1) = f(u(i)).$$

The element $u(0) \in R$ is called an *initial filling*.

Let $J = \pi R$ be the *nil-radical* of the ring R, n be the nilpotency index of R, G_f be the *graph of transformation* $f(x)$. The vertices of graph G_f lying on a cycle are called *cyclic*. A cyclic vertex a is said to be *singular* it the relations

$$f'(a) \equiv 0 \,(\mathrm{mod}\, J),$$

is satisfied and *nonsingular* otherwise. A cycle is said to be *nonsingular* if all its vertices are nonsingular. A cycle is said to be *singular* if there is a singular vertex among its vertices.

The *norm* of element $r \in R$ is the maximal $k \in \{0, 1, \ldots, n\}$ with property $r \in \pi^k R$. Let e be the unit of the ring R, $\varepsilon = \|pe\|$. Value ε is called the *ramification index* of the ring R.

Let $\circ$ be the *composition operation*, $f^{[0]} = 1$,

$$f^{[m]} = f \circ f \circ \ldots \circ f,$$

where f is repeated m times. Everywhere further vertex a belongs to a nonsingular cycle. Let $t_s(a)$ be a minimal natural number t with property

$$f^{[t]}(a) \equiv a \,(\mathrm{mod}\, J^s).$$

It's obvious that $t_s \mid t_{s+1}$ for all $s \in \{1, \ldots, n-1\}$. Our aim is to describe the sequence

$$t_1(a),\ t_2(a),\ \ldots,\ t_n(a).$$

Let φ be the natural epimorphism $R \to \bar{R} = R/pR$, $\bar{\alpha} \in \bar{R}$ ($\bar{f} \in \bar{R}[x]$) be the image of $\alpha \in R$ ($f(x) \in R[x]$) under the action of φ. We introduce the following notation.

$$\forall s \in \{1, 2, \ldots, n\}: \quad F_s = f^{[t_s(a)]}, \quad \alpha_s = F_s'(a) \in R^*,$$

$$\forall s \in \{1, 2, \ldots, n-1\}: \quad d_s(a) = t_{s+1}(a)/t_s(a),$$

$$\sigma = \min\{s \in \{1, 2, \ldots, n\} \ : \ \bar{\alpha}_s = \bar{e}\},$$

$$\forall s \in \{1, 2, \ldots, \sigma - 1\}: \quad \delta_s(a) = \operatorname{ord} \bar{\alpha}_s.$$

The following theorem holds.

Theorem 1. *The following statements are true:*

1. $d_1(a) \cdot d_2(a) \cdots d_{\sigma-1}(a) \mid \delta_1(a)$,
2. *if* $\epsilon = \min\{\varepsilon, p-1\}$, *then*

$$d_\sigma(a) \cdot d_{\sigma+1}(a) \ldots d_{n-1}(a) \mid p^{\nu(a)},$$

where

$$\nu(a) = \lceil (n - 2^\rho \sigma)/\epsilon \rceil + \rho$$

and $\rho \in \mathbb{N}_0$ *is the minimal number with property*

$$2^\rho \sigma > \epsilon.$$

In particular

$$t_n(a) \mid t_1(a) \cdot \delta_1(a) \cdot p^{\nu(a)}.$$

Let R be a finite chain ring that is not a Galois ring, $L(G_f)$ be the maximum length of cycles of transformation f, $p = \operatorname{Char} \bar{R}$, $\varepsilon = \|pe\|$. The following theorems hold.

Theorem 2. *Suppose $n \geq 4$. If $q \neq p > 2$, then*

$$L(G_f) \leq L(G_{\bar{f}}) \cdot (q-1) \cdot p^{\left[\frac{n}{2}\right]+1}.$$

If $q = p > 2$, then

$$L(G_f) \leq L(G_{\bar{f}}) \cdot p^{\left[\frac{n}{2}\right]+2}.$$

Theorem 3. *Suppose $n \geq 5$, $\sigma \in \{1, 2\}$. If $q = p = 2$, then*

$$t_n(a) \leq 2^{n-\varepsilon+1+[\log_2 \varepsilon]}.$$

If $q > p = 2$, then

$$t_n(a) \leq q \cdot (q-1) \cdot 2^{n-\varepsilon+[\log_2(\varepsilon-1)]}.$$

Let $BP(R)$ be the set of all bijective polynomial transformations of R and

$$L(R) = \max_{f \in BP(R)} L(G_f).$$

Suppose $n \geq 5$, $R_1 = GR(q^n, p^n)$. Let R be a finite chain ring with the properties $\bar{R} = GF(q)$ and $\varepsilon \geq 2$. The table below is organized as follows. The first column indicates the case in question, the second column indicates the exact value of $L(R_1)$, and the third column indicates the upper bounds for $L(R)$.

	R_1	R
$p = 2,\ q = p$	2^n	2^{n-1}
$p = 2,\ q > p$	$q \cdot (q-1) \cdot 2^{n-2}$	$q \cdot (q-1) \cdot 2^{n-3}$
$p > 2,\ q = p$	p^n	$p^{\left[\frac{n}{2}\right]+3}$
$p > 2,\ q > p$	$q \cdot (q-1) \cdot p^{n-2}$	$q \cdot (q-1) \cdot p^{\left[\frac{n}{2}\right]+1}$

Theorem 4. *Let $n \geq 7$, $R_1 = GR(q^n, p^n)$, R be a finite chain ring with the properties $\bar{R} = GF(q)$. Then $L(R) \leq L(R_1)$. Equality $L(R) = L(R_1)$ is satisfied if and only if $R \cong R_1$.*

Let's consider the multidimensional polynomial transformations. Suppose $m \geq 2$, $\mathbf{z} = (z_1, z_2, \ldots, z_m)$,

$$f_1(\mathbf{z}), \ldots, f_m(\mathbf{z}) \in R[\mathbf{z}].$$

Let $f : R^m \to R^m$ be the transformation defined by equality

$$f(\mathbf{z}) = (f_1(\mathbf{z}), \ldots, f_m(\mathbf{z})).$$

We will assume that f is a bijective transformation.

Let $L_m(R)$ be the maximum length of cycles of bijective polynomial transformations of Galois ring $R = GR(q^n, p^n)$. If R is not a finite field or a residue ring, then

$$L_m(R) = q^m(q^m - 1)p^{n-2}.$$

Suppose $\mathbf{x} \in R^m$. Let $\tau_s = \tau(F, s, \mathbf{x})$ be the period of the sequence

$$\mathbf{x} \bmod p^s, \quad f(\mathbf{x}) \bmod p^s, \quad f(f(\mathbf{x})) \bmod p^s, \quad \ldots,$$

$s = 1, 2, \ldots, n$. Let $J_f(\mathbf{x})$ be the Jacobi matrix:

$$J_f(\mathbf{x}) = \begin{pmatrix} \frac{\partial f_1}{\partial z_1}(\mathbf{x}) & \frac{\partial f_2}{\partial z_1}(\mathbf{x}) & \cdots & \frac{\partial f_m}{\partial z_1}(\mathbf{x}) \\ \frac{\partial f_1}{\partial z_2}(\mathbf{x}) & \frac{\partial f_2}{\partial z_2}(\mathbf{x}) & \cdots & \frac{\partial f_m}{\partial z_2}(\mathbf{x}) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial z_m}(\mathbf{x}) & \frac{\partial f_2}{\partial z_m}(\mathbf{x}) & \cdots & \frac{\partial f_m}{\partial z_m}(\mathbf{x}) \end{pmatrix}.$$

Suppose $F_s = f^{[\tau_s]}$, $s = 1, 2, \ldots, n$. The matrix $J(\mathbf{x}) = J_{F_1}(\mathbf{x})$ is reversible. Let $\operatorname{ord}_p J(\mathbf{x})$ be the multiplicative order of the matrix $\overline{J(\mathbf{x})}$. The following theorem holds.

Theorem 5. *Suppose* $\tau(f,1,\mathbf{x}) = q^m$. *The following statements are equivalent.*

1) $\tau(f,2,\mathbf{x}) = q^m(q^m-1)$.

2) $\operatorname{ord}_p J(\mathbf{x}) = q^m - 1$ *for all* $\mathbf{x} \in R^m$.

3) *There exists* $\mathbf{x} \in R^m$ *such that* $\operatorname{ord}_p J(\mathbf{x}) = q^m - 1$.

For every $i \in \{1,2,\ldots,m\}$ consider the matrix

$$f_i''(\mathbf{z}) = \begin{pmatrix} \frac{\partial^2 f_i(\mathbf{z})}{\partial z_1^2} & \frac{\partial^2 f_i(\mathbf{z})}{\partial z_1 \partial z_2} & \ldots & \frac{\partial^2 f_i(\mathbf{z})}{\partial z_1 \partial z_m} \\ \frac{\partial^2 f_i(\mathbf{z})}{\partial z_2 \partial z_1} & \frac{\partial^2 f_i(\mathbf{z})}{\partial z_2^2} & \ldots & \frac{\partial^2 f_i(\mathbf{z})}{\partial z_2 \partial z_m} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 f_i(\mathbf{z})}{\partial z_m \partial z_1} & \frac{\partial^2 f_i(\mathbf{z})}{\partial z_m \partial z_2} & \ldots & \frac{\partial^2 f_i(\mathbf{z})}{\partial z_m^2} \end{pmatrix}.$$

Suppose $p > 2$. If $\tau(f,n,\mathbf{x}) = L_m(R)$ for some $\mathbf{x} \in R^m$, we call f a transformation with a cycle of maximum length (CML-transformation).

We introduce the notation:

$$\forall \mathbf{x},\mathbf{y} \in R^m: \quad d^2 f(\mathbf{x},\mathbf{y}) = (\mathbf{y} f_1''(\mathbf{x})\,\mathbf{y}^T,\ \mathbf{y} f_2''(\mathbf{x})\,\mathbf{y}^T,\ \ldots,\ \mathbf{y} f_m''(\mathbf{x})\,\mathbf{y}^T),$$

where "T" is the transpose operation.

Suppose $\tau(f,2,\mathbf{x}) = q^m(q^m-1)$. For every $k \geq 1$ we denote the matrix

$$(J(\mathbf{x}) - E)^{-1} \cdot (J(\mathbf{x})^k - E)$$

by $A^{[k]}(\mathbf{x})$. Suppose $B^{[1]}(\mathbf{x},\mathbf{y}) = 0$,

$$B^{[j]}(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{j-1} d^2 F_1(\mathbf{x}, \mathbf{y} A^{[k]}(\mathbf{x})) J(\mathbf{x})^{j-1-k}$$

for all $j \geq 2$, $\mathbf{y} \in R^m$.

Theorem 6. *Suppose* $p > 2$, $\tau(f, 2, \mathbf{x}) = q^m(q^m - 1)$, $F_1(\mathbf{x}) = \mathbf{x} + p\mathbf{y}$. *Then* f *is a CML-transformation if and only if*

$$\mathbf{y}\gamma_1\left[A^{[q^m-1]}(\mathbf{x})\right] + \frac{1}{2}B^{[q^m-1]}(\mathbf{x}, \mathbf{y}) \not\equiv 0 \,(\mathrm{mod}\, pR),$$

where $\gamma_1[\bullet]$ *is the first digit in the Teichmüller decomposition.*

On the basis of the theorem 6 an algorithm is proposed that allows constructing pairs $(f, \mathbf{x})$ with property

$$\tau(f, n, \mathbf{x}) = L_m(R) = q^m(q^m - 1)p^{n-2}.$$

For some of these CML-transformations f, it is possible to describe their cyclic structures.

Let Ω be a nonempty finite set. The cyclic structure of an arbitrary permutation $\psi \in S(\Omega)$ is described by its cyclic type, that is, the polynomial

$$C_\psi(y) = \sum_{i \geq 1} c_i(\psi) y^i \in \mathbb{Z}[y],$$

where $c_i(\psi)$ is the number of cycles with length i. Consider the polynomial

$$C_{m,R}(y) = y + \sum_{s=0}^{n-1} \left(\frac{q^m}{p}\right)^{n-s-1} y^{(q^m-1)p^{n-s-1}}.$$

We managed to construct a large class of transformations f with the property:

$$C_f(y) = C_{m,R}(y^{q^m}).$$

Almost all cycles of such transformations f have length $L_m(R)$.

k-linear shift register

Let's discuss the self-controlled 2-LFSR and list the main results concerning this issue. Let I be a monic ideal of the ring $R[x_1, x_2, \ldots, x_k]$ and u be a k-linear recurring sequence (k-LRS) annihilated by an ideal I. We denote the set of all such sequences u by $L_R(I)$. If $T(I)$ is the period of the ideal I and $T(u)$ is the period of the sequence u, then the inequality holds: $T(u) \leq T(I)$. In some special cases, the cyclic structure of the set $L_R(I)$ is described. A large family of sequences u possessing property $T(u) = T(I)$ is constructed. Everywhere further $T(u) = T(I)$ and the sequence u specifies the initial filling of the self-controlled 2-LFSR. Let β be the control function of this automation, ψ be the output function, γ be the output sequence. Large classes of functions β and ψ are constructed for which $T(\gamma) = T(u)$. For functions β and ψ from these classes, some cryptographic properties of the output sequence γ are described (the periodical properties, the statistical properties and the linear complexity).

Let's describe the results in more detail. Informally, 2-LFSR can be described as follows. Let R be a finite commutative ring with identity. Let $F_0(x)$ and $F_1(x)$ be monic polynomials of degrees m_0 and m_1, respectively. Suppose $w(0) \in R_{m_0,m_1}$. Consider a mapping

$$\mu : \mathbb{N}_0^2 \to R$$

such that

$$\mu[\overline{0, m_0 - 1} \times \overline{0, m_1 - 1}] = w(0),$$

and in the table, each column is a linear recurring sequence (LRS) with characteristic polynomial $F_0(x)$ and each line is an LRS with characteristic polynomial $F_1(x)$:

$\mu(0,0)$	$\mu(0,1)$	$\mu(0,2)$	$\dots$	$\mu(0,j)$	$\dots$
$\mu(1,0)$	$\mu(1,1)$	$\mu(1,2)$	$\dots$	$\mu(1,j)$	$\dots$
$\mu(2,0)$	$\mu(2,1)$	$\mu(2,2)$	$\dots$	$\mu(2,j)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\mu(i,0)$	$\mu(i,1)$	$\mu(i,2)$	$\dots$	$\mu(i,j)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

We call such a mapping μ 2-linear recurring sequence (2-LRS). We denote the set of all such 2-LRS μ by $L_R(F_0, F_1)$.

A rectangular window $m_0 \times m_1$ moves along the table. The current filling $w(i)$ of the window is the current filling of the register. We will adhere to the following agreements.

1. The law of movement of the window is given by a binary *control sequence* δ. If $\delta(i) = 0$, then the window is moved one step down. If $\delta(i) = 1$, then the window is moved one step to the right.

2. Either the sequence δ is the input, or the sign $\delta(i)$ is obtained from the current filling $w(i)$ using a *control function* β:
$$\delta(i) = \beta(w(i)), \quad i = 0, 1, 2, \dots$$
In the first case, the automation is called non-autonomous and is denoted by $\mathfrak{A}$. In the second case, the automation is called self-controlled and is denoted by $\mathfrak{A}^{\beta}$.

3. The output sign $\gamma(i)$ is obtained from the current filling $w(i)$ using a linear *output function* ψ:
$$\gamma(i) = \psi(w(i)), \quad i = 0, 1, 2, \dots$$

Let φ_0 and φ_1 be the partial transfer functions of the automation $\mathfrak{A}$:
$$w(i+1) = \varphi_{\beta(w(i))}(w(i)).$$

Suppose $r, n \in \mathbb{N}$, $R = GR(q^n, 2^n)$, $q = 2^r$, $m \geq 2$, $F_0(x) = F_1(x) = F(x)$ is a polynomial of maximal period $(q^m - 1)2^{n-1}$, $\deg F(x) = m$. We will assume that the output function ψ returns the content of some fixed cell of the argument matrix:

$$\psi(z) = z_{k,l},$$

where $z = (z_{i,j}) \in R_{m,m}$.

Suppose that $\tau = q^m - 1$ and the automorphism σ of the R-bimodule $R_{m,m}$ is determined by the equality:

$$\sigma = \varphi_0^{2^{n-2}(\tau-1)} \cdot \varphi_1^{2^{n-2}(\tau+1)}.$$

Let θ be a root of the polynomial F in the ring $S = GR(q^{mn}, 2^n)$. Suppose $\alpha = \theta^{2^{n-2}(\tau-1)}$ and $\mu_j(x)$ is the minimal polynomial of $\bar{\alpha}^{q^j-1}$ over the field $\bar{R}$, $j = 1, 2, \ldots, m-1$. Then the characteristic polynomial of σ has the following canonical decomposition:

$$\chi_\sigma(x) = G_0(x)G_1(x)\ldots G_{m-1}(x),$$

where $\bar{G}_0(x) = (x-1)^m$, $\bar{G}_j(x) = \mu_j(x)$, $j = 1, 2, \ldots, m-1$. This decomposition induces the following unambiguous representation of every state w of the automation $\mathfrak{A}^\beta$:

$$w = a_0 + a_1 + a_2 + \ldots + a_{m-1},$$

where $a_j \in \mathrm{Ker}\ G_j(\sigma)$, $j = 0, 1, \ldots, m-1$. We call the *type* of state w the following vector:

$$\mathrm{typ}\, w = (n - \|a_0\|, n - \|a_1\|, \ldots, n - \|a_{m-1}\|) \in \{0, 1, \ldots, n\}^m.$$

If $e_{i,j}$ is a matrix unit ($i, j \in \{1, 2, \ldots, m\}$), then the equality holds:

$$a_0 = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} u(i+j) e_{i,j},$$

where $u \in L_R(F)$. We say that the sequence u is *associated* with the matrix w.

Let's construct the control function β. Every function $f : \bar{R}^m \to \mathbb{Z}_2$ with property $f(0, 0, \ldots, 0) = 0$ is comparable to its weight

$$|f| = |\{\alpha \in \bar{R}^m \ : \ f(\alpha) = 1\}|.$$

We consider a mapping ξ associating with each set $\mathbf{t} \in \{0, 1, \ldots, n\}^m$ a certain function $\xi(\mathbf{t}) = f_{\mathbf{t}}$ with the property $(|f_{\mathbf{t}}|, \tau) = 1$. If $w \in R_{m,m}$ and $\mathbf{t} = \operatorname{typ} w$ then put

$$\beta(w) = f_{\mathbf{t}}(\bar{u}(0), \bar{u}(1), \ldots, \bar{u}(m-1)),$$

where $u \in L_R(F)$ is the recurrence associated with w. Next, we consider only initial fillings $w = w(0)$ for which $\bar{a}_0 \neq 0$.

The phrase "the property is satisfied for almost all states" means that the fraction of states for which the property is not satisfied is $o(1)$, $m \to \infty$. Let ε_j be the indicator of property $a_j \neq 0$, $j = 1, 2, \ldots, m-1$. The following statements are true:

1. If $\tau_j = \tau/(q^{(m,j)} - 1)$, $j = 1, 2, \ldots, m-1$, then

$$T(\gamma) = 2^{n-1}\tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \ldots, \tau_{m-1}^{\varepsilon_{m-1}}] \leq 2^{n-1} \cdot \frac{\tau^2}{q-1}. \tag{1}$$

2. Inequality (1) turns into equality if and only if

$$(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \ldots, (m-1)\varepsilon_{m-1}, m) = 1.$$

For almost all initial fillings $w(0)$ the following relation holds:

$$T(\gamma) = O(q^{2m}), \quad m \to \infty.$$

3. The number $N(\mathfrak{A}^\beta)$ of initial states for which

$$T(\gamma) = 2^{n-1} \cdot \frac{\tau^2}{q-1}$$

is expressed by the formula:

$$N(\mathfrak{A}^\beta) = (q^m - 1) \sum_{d|m} \mu(m/d) q^{m(nd-1)},$$

where μ is Möbius function. Almost all initial states belongs to cycles of maximum length.

Suppose $t = \min\{\|a_1\|, \|a_2\|, \ldots, \|a_{m-1}\|\}$. Consider the Teichmüller decomposition of the output sequence γ:

$$\gamma = \gamma_0 + 2\gamma_1 + \ldots + 2^{n-1}\gamma_{n-1}.$$

Let's study the linear complexity (rank) and the statistical properties of the sequence γ_t. Let $p_z(\gamma_t)$ be the relative frequency of the appearance of the element z on the cycle of the sequence γ_t.

The following statements are true:

1. If $J = \{j \in \overline{1, m-1} : \|a_j\| = t\}$, then there exists LRS $u \in L_R(F)$ such that $\bar{u} \neq 0$ and the following inequality holds:

$$m \cdot \sum_{j \in J} \tau_j \leq \text{rang } \gamma_t - \text{rang } u_t \leq m \cdot |J| \cdot \tau,$$

where u_t is the digit number t in the Teichmüller decomposition of u. Hence,

$$\text{rang } \gamma_t = O(m^2 q^m), \quad m \to \infty.$$

2. If $n = 1$, then

$$m + m\sum_{j=1}^{m-1} \tau_j \varepsilon_j \le \operatorname{rang} \gamma \le m + m\tau \sum_{j=1}^{m-1} \varepsilon_j.$$

If $\varepsilon_j = 1$ for all $j \in \mathbb{Z}_m^*$, then

$$\operatorname{rang} \gamma \ge m + m\varphi(m) \cdot \frac{q^m - 1}{q - 1},$$

where φ is Euler function.

3. Suppose $\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{m-1} = 1$, $t = \|a_j\|$, $q > 2$,

$$C = \left(\frac{q-1}{q-2}\sqrt{q} + \frac{q-1}{q^{(m,j)} - 1}\right) \cdot \left(1 + \frac{\sqrt{q}}{q-2}\right)^{-1},$$

and the state $w(0)$ belongs to a cycle of maximal length. Then for every $z \in \bar{R} = GF(q)$ following statements are true:

a) if $(q - 1, \tau_j) < C$, then

$$\left| p_z(\gamma_t) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| < \frac{1}{2(q^m - 1)} + \frac{(\sqrt{q} + 1)(q-1)}{q^m - 1} q^{m/2-1},$$

b) if $(q - 1, \tau_j) \ge C$, then

$$\left| p_z(\gamma_t) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| < \frac{1}{2(q^m - 1)} + \frac{(q-1)^2}{q^m - 1} q^{m/2-1}.$$

4. Suppose $\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{m-1} = 1$, $t = \|a_j\|$ and $(q - 1) \mid \tau_j$. Then

$$\forall z \in \bar{R} : \left| p_z(\gamma_t) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q\tau^2} \right| \le \frac{1}{2\tau} + \frac{q-1}{q} \cdot \left(\frac{1}{\tau_j} - \frac{1}{\tau}\right) \cdot q^{m/2}.$$

Suppose $R = \mathbb{Z}_2$, $\vec{w} = (w(0), w(1), \ldots, w(i), \ldots)$. It is obvious that $T(\vec{w}) \leq \tau^2$. A function

$$\beta : R_{m,m} \to \mathbb{Z}_2$$

is said to be *optimal* if, under condition $a_0 \neq 0$, the equality $T(\vec{w}) = \tau^2$ is equivalent to the condition

$$(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \ldots, (m-1)\varepsilon_{m-1}, m) = 1.$$

Let's describe the optimal functions β.

A *loop* containing the recurrence $\mu \in L_R(F, F)$ is the set

$$C = C(\mu) = \{x_0^{t_0} x_1^{t_1} \mu \mid (t_0, t_1) \in \mathbb{N}_0^2\}.$$

The LRS-family $L_R(F, F)$ splits into cycles. Suppose

$$\mathfrak{F} = \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, m-1\}.$$

If the recurrences μ_1 and μ_2 belong the same cycle, then

$$\operatorname{typ} \mu_1[\mathfrak{F}] = \operatorname{typ} \mu_2[\mathfrak{F}].$$

A *type* of the cycle C is the vector $\operatorname{typ} C = \operatorname{typ} \mu[\mathfrak{F}]$. Suppose

$$C[\mathfrak{F}] = \{\mu[\mathfrak{F}] \mid \mu \in C\},$$

V is the set of binary vectors $(1, c_1, c_2, \ldots, c_{m-1})$ such that

$$(c_1, 2c_2, 3c_3, \ldots, (m-1)c_{m-1}, m) = 1.$$

Theorem 7. *The control function β is optimal if and only if for every cycle $C \subset L_R(F,F)$ with property* $\operatorname{typ} C \in V$ *there exists a boolean function $f(x_1, x_2, \ldots, x_m)$ such that*

$$f(0,0,\ldots,0) = 0, \quad (|f|,\tau) = 1$$

and

$$\forall\, w \in C[\mathfrak{F}]: \quad \beta(w) = f(u(0), u(1), \ldots, u(m-1)),$$

where $u \in L_R(F)$ is LRS associated with w.

Let $\psi_{i,j} : R_{m,m} \to R$ be the function determined by equation

$$\forall\, z \in R_{m,m}: \quad z = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \psi_{i,j}(z) e_{i,j}.$$

There exists $t \in \{1, 2, \ldots, m^2\}$ and the set of pair

$$(i_1, j_1),\ (i_2, j_2),\ \ldots,\ (i_t, j_t) \in \mathfrak{F}$$

such that

$$\psi = \sum_{k=1}^{t} \psi_{i_k, j_k}.$$

Suppose $s \in \{0, 1, \ldots, m-1\}$. Consider the polynomial

$$\chi_s(x) = \sum_{k=1}^{t} x^{2^s i_k + j_k} \in R[x].$$

The *type* of the linear function ψ is the vector $\operatorname{typ}\psi = (\varepsilon'_0, \varepsilon'_1, \ldots, \varepsilon'_{m-1})$, where

$$\forall s \in \{0, 1, \ldots, m-1\}: \quad \varepsilon_s = \begin{cases} 0, & \text{if } F(x) \mid \chi_s(x), \\ 1 & - \text{ otherwise.} \end{cases}$$

Theorem 8. *Suppose that β is optimal,*

$$\operatorname{typ} w(0) = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1}) \in V,$$

ψ is a linear function, $\operatorname{typ} \psi = (\varepsilon'_0, \varepsilon'_1, \ldots, \varepsilon'_{m-1})$,

$$\lambda_s = \varepsilon'_s \varepsilon_s, \quad s = 0, 1, \ldots, m-1.$$

Then

$$T(\gamma) = [\tau^{\lambda_0}, (\tau\tau_1)^{\lambda_1}, (\tau\tau_2)^{\lambda_2}, \ldots, (\tau\tau_{m-1})^{\lambda_{m-1}}],$$

where $\tau_s = \tau/(2^{(m,s)} - 1)$, $s = 1, 2, \ldots, m-1$. The equality $T(\gamma) = \tau^2$ holds if and only if

$$(\lambda_1, 2\lambda_2, \ldots, (m-1)\lambda_{m-1}, m) = 1.$$

If $\nu \in L_R(F, F)$, then we call the length of the cycle $C(\nu)$ the value $T(\nu) = |C(\nu)|$, that is, the *period* of the sequence ν. The *cyclic type* of the family $L_R(F, F)$ is the polynomial

$$C_F(y) = \sum_{t \geq 1} C_{F,t} \cdot y^t,$$

where $C_{F,t}$ is the number of cycles of length t in the family $L_R(F, F)$.

Theorem 9. *Suppose $R = \mathbb{Z}_2$, $F(x)$ is a polynomial of maximal period $\tau = 2^m - 1 \geq 3$ and $\tau_d = \tau/(2^d - 1)$ for every $d \mid m$. Then:*

1. *If $m = d_1 > d_2 > d_3 > \ldots > d_l = 1$ are all natural divisors of m, then the lengths of the cycles of the family $L_R(F, F)$ form the series*

$$1 < \tau = \tau\tau_{d_1} < \tau\tau_{d_2} < \ldots < \tau\tau_{d_l} = \tau^2.$$

2. *Suppose* $\nu \in L_R(F,F)$ *and* $\operatorname{typ}\nu[\mathfrak{F}] = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1})$. $T(\nu) = 1$ *if and only if* $\nu = 0$. $T(\nu) = \tau\tau_d$ *if and only if*

$$\nu \neq 0 \ \text{ and } \ (\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \ldots, (m-1)\varepsilon_{m-1}, m) = d.$$

3. *The cyclic type* $C_F(y)$ *of the family* $L_R(F,F)$ *is expressed by the formula*

$$C_F(y) = y + y^{\tau} + \sum_{d|m,\, d<m} (\tau\tau_d)^{-1} \sum_{t|\frac{m}{d}} \mu\left(\frac{m}{dt}\right) 2^{mt} y^{\tau\tau_d},$$

where μ *is Möbius function.*

Let's consider the k-dimensional case in situation $k \geq 3$. Let

$$F_0(x),\ F_1(x),\ \ldots,\ F_{k-1}(x)\ \in R[x] \tag{2}$$

be the polynomials of maximal period,

$$\deg F_0(x) = \deg F_1(x) = \ldots = \deg F_{k-1}(x) = m \geq 2.$$

Let $I \lhd R_k = R[x_0, x_1, \ldots, x_{k-1}]$ be the ideal generated by the polynomials (2):

$$I = (F_0(x_0), F_1(x_1), \ldots, F_{k-1}(x_{k-1}))_{R_k}.$$

We call a *k-sequence* any mapping $u : \mathbb{N}_0^k \to R$. We denote the set of all k-sequences by $R^{\langle k\rangle}$. We endow the set $R^{\langle k\rangle}$ with the structure of R_k-module:

$$(ax_0^{t_0}x_1^{t_1}\ldots x_{k-1}^{t_{k-1}} \cdot u)(i_0, i_1, \ldots, i_{k-1}) = au(i_0 + t_0, \ldots, i_{k-1} + t_{k-1}).$$

Let $L_R(I)$ be the set of those sequences u that are annihilated by all polynomials in the ideal I. Such sequences u will be called *k-linear recurring sequences* (k-LRS) with monic characteristic ideal I. Suppose $u \in L_R(I)$. A *cycle* containing k-LRS u will be called the set

$$C(u) = \{x_0^{t_0}x_1^{t_1}\ldots x_{k-1}^{t_{k-1}} \cdot u \mid (t_0, t_1, \ldots, t_{k-1}) \in \mathbb{N}_0^k\}.$$

The quantity $T(u) = |C(u)|$ is called the *period* of k-LRS u. We introduce the concept of period of ideal I. *A group of vector-periods* of ideal I is the subgroup $\mathfrak{P}(I)$ of $(\mathbb{Z}^k, +)$ generated by vectors

$$\mathbf{t} = (t_0, t_1, \ldots, t_{k-1}) \in \mathbb{N}_0^k$$

having the property $\mathbf{x}^{\mathbf{t}} - 1 \in I$, where $\mathbf{x}^{\mathbf{t}} = x_0^{t_0} x_1^{t_1} \ldots x_{k-1}^{t_{k-1}}$. The *period* $T(I)$ of ideal I is the index $|\mathbb{Z}^k : \mathfrak{P}(I)|$ of the subgroup $\mathfrak{P}(I)$ in the group $\mathbb{Z}^k$. The following relation holds:

$$\forall\, u \in L_R(I): \quad T(u) \mid T(I)\,.$$

We call k-LRS $u \in L_R(I)$ *quasi-maximal* if $T(u) = T(I)$. Let R be a finite field $GF(q)$. The following theorems hold.

Theorem 10. *Suppose* $R = \mathrm{GF}(q)$, $k \geq 3$, $m \geq 1$, *the polynomials* (2) *are the polynomials of maximal period, the ideal* $I \lhd R_k$ *is generated by the polynomials* (2). *In the family* $L_R(I)$ *there are quasi-maximal recurrences if and only if*

$$(\tau, (q-1)^2) = q - 1. \tag{3}$$

Under condition (3), *the fraction of quasi-maximal recurrences among all recurrences of the family* $L_R(I)$ *at least* $(1 - q^{-m})^k$.

Theorem 11. *Under the conditions of the theorem* 10 *and if condition* (3) *is satisfied, there are at least*

$$(q-1)^{k-1} q^{m^k - mk}$$

cycles of the maximum possible length $T(I)$ *in the family* $L_R(I)$.

Conclusion

The researches have shown that the considered automata can be useful at synthesis of generators of pseudo-random sequences. The author is grateful to doctor I.A. Kruglov for attention to this work and to doctor V.E. Viktorenkov for useful discussions.