Математичний Вісник
Наукового товариства
імені Шевченка
2013. — Т.10

Mathematical Bulletin
of the Shevchenko
Scientific Society
2013. — V.10

LINEAR-INVERSIVE GENERATOR OF PRN'S WITH A VARIABLE MULTIPLIER

Tran The Vinh, Pavel Varbanets

Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine

Tran The Vinh, Pavel Varbanets, *Linear-inversive generator of PRN's with a variable multiplier*, Math. Bull. Shevchenko Sci. Soc. **10** (2013), 75–84.

A new linear-inversive congruential generator of pseudorandom numbers (PRN's) with a variable multiplier is introduced. It is proved that the sequence of PRN's produced by such generator passes the 4-dimensional serial test on statistical independency.

Тран Тхе Вінь, Павло Варбанець. *Лінійно-інверсний генератор ПВЧ із змінним множником* // Мат. вісник НТШ. — 2013. — Т.10. — С. 75–84.

У статті представлено новий лінійно-інверсний конгруентний генератор псевдовипадкових чисел із змінним множником. Доведено, що послідовність псевдовипадкових чисел, породжена таким генератором, проходить 4-вимірний серіальний тест на статистичну незалежність.

Introduction

Let p be a prime number, $m > 1$ be a positive integer. Consider the following recursion

$$y_{n+1} \equiv a y_n^{-1} + b \pmod{p^m}, \quad (a, b \in \mathbb{Z}), \tag{1}$$

where y_n^{-1} is a multiplicative inverse $\bmod\, p^m$ for y_n if $(y_n, p) = 1$. The parameters a, b, y_0 we be called the multiplier, shift and initial value, respectively.

In [3], [4], [6], [7], [8], [11], [12], [14] it was proved that under certain conditions on the parameters a, b, y_0 the inversive congruential generator (1) produces a sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$, $n \geq 0$, which passes s-dimensional serial tests on equidistribution and statistical independence for $s \in \{1, 2, 3, 4\}$.

2010 *Mathematics Subject Classification:* 11L07; 45B67, 11T23, 11T71, 11K45 *УДК:* 511.33
Key words and phrases: linear-inversive congruential generator, statistical independency, pseudorandom numbers, exponential sum, discrepancy
E-mail: ttvinhcntt@yahoo.com.vn, varb@sana.od.ua

It turns out that this generator is extremely useful for Quasi-Monte Carlo type application (see [5], [13]). The sequences of PRN's can be used for the cryptographic applications. In this case the initial value y_0 and the constants a and b are assumed to be a secret key, and the output of the generator (1) can be used as a stream cipher. Observe that for determining the parameters a and b of the generator (1) it is enough to recognize two successive elements y_n, y_{n+1} generated by (1). Moreover, according to [1], [2], the reconstruction of generator (1) can be obtained if we know some sequence of "approximations" to $y_n, y_{n+1}, \ldots, y_{n+k}$. Thus one should be careful using the generator (1) for cryptographic purposes.

The main point of our further presentation in a generalization of the generator (1). We consider the following recursive relation

$$y_{n+1} \equiv a y_n^{-1} + b + cF(n) y_n \pmod{p^m} \tag{2}$$

under the conditions $(a, p) = (y_0, p) = 1$, $b \equiv c \equiv 0 \pmod p$, $F(u)$ is a polynomial over $\mathbb{Z}[u]$.

The generator (2) will be called the linear-inversive generator with a variable multiplier $cF(n)$. The computational complexity of the generator (2) is the same as for the generator (1), but the reconstruction of parameters a, b, c, n and polynomial $F(n)$ is a tricky problem even if the several consecutive values $y_n, y_{n+1}, \ldots, y_{n+N}$ will be revealed. Thus the generator (2) can be used in the cryptographical applications. Notice that the conditions $(a, p) = (y_0, p) = 1$, $b \equiv c \equiv 0 \pmod p$ guarantee that the recursion (2) produces an infinite sequence $\{y_n\}$.

The purpose of this work is to show that the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$, passes the test on equidistribution and statistical independence, which makes possible to use such sequences in the problems of real processes modeling and cryptography.

Notations: For p being a prime number, put

$$\begin{aligned} &R_m := \{0, 1, \ldots, p^m - 1\}; \quad R_m^* := \{a \in R_m \mid (a, p) = 1\}, \\ &e_m(u) := e^{2\pi i \frac{u}{p^m}}, u \in \mathbb{R}; \quad \exp(x) := e^x \text{ for } x \in \mathbb{R}, \\ &\nu_p(A) = \alpha \in \mathbb{N} \cup \{0\} \text{ if } p^\alpha \parallel A \text{ and } p^{\alpha+1} \nmid A. \end{aligned}$$

For $u \in \mathbb{Z}$, $(u, p) = 1$ we write u^{-1} if $u \cdot u^{-1} \equiv 1 \pmod{p^m}$.

1. Auxiliary results

Let $f(x)$ be a periodic function with period τ. For any $N \in \mathbb{N}$, $1 \leq N \leq \tau$, we denote

$$S_N(f) := \sum_{x=1}^{N} e^{2\pi i f(x)}$$

We will need the following well-known statements.

Lemma 1.1 ([9]). $|S_N(f)| \leq \max_{1 \leq n \leq \tau} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(f(x) + \frac{nx}{\tau}\right)} \right| \log \tau.$

Let $\mathfrak{I}(A, B; p)$ be the number of solutions of the congruence $A - Bu^2 \equiv 0 \pmod p$, $(u, p) = 1$.

Lemma 1.2 ([16]). *Let p be a prime number and let $f(x)$, $g(x)$ be two polynomials over $\mathbb{Z}$*

$$f(x) = A_1 x + A_2 x^2 + p(A_3 x^3 + \cdots), \quad g(x) = B_1 x + p(B_2 x^2 + \cdots),$$

and, moreover, let $\nu_p(A_2) = \alpha > 0$, $\nu_p(A_j) \geq \alpha$ for all $j \geq 3$. Then we have the estimates

$$\Big|\sum_{x \in R_m} e_m(f(x))\Big| \leq \begin{cases} 2p^{\frac{m+\alpha}{2}} & \text{if } \nu_p(A_1) \geq \alpha, \\ 0 & \text{else}, \end{cases}$$

and

$$\Big|\sum_{x \in R_m^*} e_m(f(x) + g(\overline{x}))\Big| \leq \begin{cases} (\Im(A_1, B_1; p) \cdot p)^{\frac{m}{2}} & \text{if } (B_1, p) = 1, \\ 2p^{\frac{m+\alpha}{2}} & \text{if } \nu_p(A_1) \geq \alpha,\ \nu_p(B_j) \geq \alpha \text{ for all } j \geq 1, \\ 0 & \text{if } \nu_p(A_1) < \alpha \leq \nu_p(B_j) \text{ for all } j \geq 1. \end{cases}$$

2. Preparations

Consider the sequence $\{y_n\}$ produced by the recursion (2).

Let $n = 2k$. We put

$$y_{2k} \equiv \frac{a_0^{(k)} + a_1^{(k)} y_0 + \cdots}{b_0^{(k)} + b_1^{(k)} y_0 + \cdots} := \frac{A_k}{B_k} \pmod{p^m} \tag{3}$$

Twice using the recursion (2) we infer

$$y_{2(k+1)} = \frac{A_{k+1}}{B_{k+1}} = \frac{aA_k^2 B_k^2 + bA_k B_k (aB_k^2 + bA_k B_k + cF(2k)A_k^2) + D(a,b,c,k)}{A_k B_k (aB_k^2 + bA_k B_k + cF(2k)A_k^2)}, \tag{4}$$

where

$$D = cF(2k{+}1)\left(a^2 B_k^4 + b^2 A_k^2 B_k^2 + c^2 F^2(2k) A_k^4 + 2abA_k B_k^5 + 2acF(2k) A_k^2 B_k^2 + 2bcF(2k) A_k^3 B_k\right).$$

Define the following matrices

$$\begin{aligned} S_0 &= \begin{pmatrix} a{+}b^2{+}cb^2F(2k{+}1){+}2ac^2F(2k)F(2k{+}1) & ab(1{+}2cF(2k{+}1){+}a^2cF(2k{+}1)) \\ b & a \end{pmatrix}, \\ S_1 &= \begin{pmatrix} c^3F^2(2k)F(2k+1) & 3bcF(2k) \\ 0 & cF(2) \end{pmatrix}, \end{aligned} \tag{5}$$

and vectors

$$S_2 = \begin{pmatrix} a^2cF(2k+1) \\ 0 \end{pmatrix}, \quad \widetilde{A}_k = \begin{pmatrix} A_k^4 B_k^0 \\ A_k^3 B_k \\ A_k^2 B_k^2 \\ A_k B_k^3 \\ A_k^0 B_k^4 \end{pmatrix}.$$

Now, using (3)–(5), we get

$$\begin{pmatrix} A_{k+1} \\ B_{k+1} \end{pmatrix} = T_k \begin{pmatrix} A_k \\ B_k \end{pmatrix} \tag{6}$$

where $T_k = (S_1|S_0|S_2)$ and the sign $|$ denotes concatenation of matrices.

Recursion (2) gives

$$y_0 = \frac{y_0}{1}, \quad y_1 = \frac{a + by_0 + cF(0)y_0^2}{y_0},$$
$$y_2 = \frac{y_0^2 + b(ay_0 + by_0^2 + cF(0)y_0^3) + cF(1)(a + by_0 + cF(0)y_0^2)^2}{ay_0 + by_0^2 + cF(0)y_0^3}.$$

In general case, let

$$y_{2k} \equiv \frac{\sum\limits_{\ell \geq 0} A_\ell^{2k} y_0^\ell}{\sum\limits_{\ell \geq 0} B_\ell^{2k} y_0^\ell}, \quad A_\ell^{2k}, B_\ell^{2k} \in \mathbb{Z}, \text{ and } y_{2(k+1)} \equiv \frac{\sum\limits_{\ell \geq 0} A_\ell^{2(k+1)} y_0^\ell}{\sum\limits_{\ell \geq 0} B_\ell^{2(k+1)} y_0^\ell}. \tag{7}$$

Using (2) we deduce modulo p that

$$\mathbf{A}_\ell^{\mathbf{2(k+1)}} = \sum_{s+t=\ell} \sum_{i=0}^{s} \sum_{j=0}^{t} aA_i B_{s-i} A_j B_{t-j}\ ) \quad \text{and} \quad \mathbf{B}_\ell^{\mathbf{2(k+1)}} = \sum_{\substack{s,t \geq 0 \\ s+t=\ell}} \sum_{i=0}^{s} \sum_{j=0}^{t} aB_i A_j B_{s-i} B_{t-j}.$$

Let ℓ_0 (respectively, ℓ_1) be an exponent of y_0, for which $\big(A_{\ell_0}^{(2k)}, p\big) = 1$ (respectively, $\big(B_{\ell_1}^{(2k)}, p\big) = 1$). It is easy to see that $A_i \equiv B_j \equiv 0 \pmod p$ if $i \neq \ell_0$, $j \neq \ell_1$. First, we notice that

$$\ell_0(k) := \ell_0 = \frac{2^{2k} + 2}{3} \quad \text{and} \quad \ell_1(k) := \ell_0(k) - 1 = \frac{2^{2k} - 1}{3}.$$

Indeed, for $k = 0$ this relations hold. We use induction on k. By the inductive hypothesis, in the righthand sum of the equality

$$A_\ell^{(2k+2)} = \sum_{s+t=\ell} \sum_{i=0}^{s} \sum_{j=0}^{t} aA_i B_{s-i} A_j B_{t-j} \pmod p$$

only the summand $aA_i B_{s-i} A_j B_{t-j}$ with $i = j = \frac{2^{2k}+2}{3}$ may be incongruent to $0 \pmod p$. But then we must have

$$s - i = \frac{2^{2k} - 1}{3}, \quad t - j = \frac{2^{2k} - 1}{3},$$

and these equalities uniquely define values s and t as $s = t = \frac{2^{2k+1}+1}{3}$. Hence,

$$\ell_0(k+1) = s + t = \frac{2^{2k+2} + 2}{3}.$$

The value of ℓ_1 can be determined similarly. So, the required relations for ℓ_0 and ℓ_1 are proved.

Next, we have for $k \geq 1$ that $\nu_p\big(A_\ell^{(2k)}\big) \geq \big|\frac{\ell_0 - \ell}{2}\big| \cdot \nu_p(b)$, and $\nu_p\big(B_\ell^{(2k)}\big) \geq \big|\frac{\ell_1 - \ell}{2}\big| \cdot \nu_p(b)$. Thus, for $k \geq 2m_0 + 1$, $m_0 = \big[\frac{m}{\nu_p(b)}\big]$ modulo p^m, the numerator and denominator of (7) modulo p^m contain at most $4m_0 + 1$ summands, i.e. we have

$$y_{2k} = \frac{\left(\sum\limits_{\ell=\ell_0-2m_0}^{\ell_0+2m_0} A_\ell^{(2k)} y_0^\ell\right)}{\left(\sum\limits_{\ell=\ell_1-2m_0}^{\ell_1+2m_0} B_\ell^{(2k)} y^\ell\right)}. \tag{8}$$

Multiplying the numerator and the denominator in (8) by a^{-k}, we obtain the following representation

$$y_{2k} = \frac{\sum \overline{A}_\ell y^\ell}{\sum \overline{B}_\ell y^\ell}, \quad \overline{A}_\ell \equiv \overline{a}^k A_\ell, \quad \overline{B}_\ell \equiv \overline{a}^k B_\ell \pmod{p^m}. \tag{9}$$

Here the coefficients $\overline{A}_\ell$, $\overline{B}_\ell$ are polynomials of k with coefficients depending only on a^i, b^i, c^i, $\overline{a}^i$, $1 \le i \le 2m+1$, and these coefficients have the above-indicated properties of divisibility by a power of p.

Now, using the equalities (4)–(8) and method of the proof for Proposition 1 in [15] we obtain the following:

Proposition 2.1. *Let $\{y_n\}$ be the sequence produced by (2) and let $\nu_p(b) = \nu$, $\nu_p(c) = \mu$, $\nu < \mu$. Then for $k \ge 2m+1$ we get the following congruences modulo p^m*

$$\begin{aligned} y_{2k} &= kb + \left[1 - k(k-1)a^{-1}b^2\right] y_0 + \left[-ka^{-1}b\right] y_0^2 + \\ &+ \left[k^2a^{-2}b^2 - ka^{-1}cG_0(k)\right] y_0^3 + p^\alpha H_0(k, y_0), \\ y_{2k+1} &= [a - k(k+1)b^2]y_0^{-1} - kaby_0^{-2} + k^2ab^2y_0^{-3} + kcG_1(k)y_0 + \\ &+ (kcG_2(k) + (k+1)b)\, y_0^2 + p^\alpha H_1(k, y_0), \end{aligned} \tag{10}$$

where $\alpha = \min(2\nu, \mu)$, $G_i(k)$, $i = 1, 2, 3$ are polynomials from $\mathbb{Z}[k]$, $H_0(k, y_0), H_1(k, y_0) \in \mathbb{Z}[k, y_0]$, and the coefficients $G_i(k)$, $H_0(k, y_0)$, $H_1(k, y_0)$ depend only on $a^i, a^{-i}, b^i, c^i \pmod{p^m}$, $i = 1, \ldots, 2m+1$.

Corollary 2.2. *Let the conditions of Proposition 2.1 are satisfied. Then for $p > 2$ the sequence $\{y_n\}$ is purely periodic with period $2p^{m-\ell}$, where*

$$\ell = \begin{cases} \nu_p(b) + \nu_p(a - y_0^2) & \text{if } \nu_p(a - y_0^2) < \nu_p(b) \le \frac{1}{2}m; \\ 2\nu_p(b) & \text{if } \nu_p(a - y_0^2) > \nu_p(b),\ \nu_p(b) \le \frac{1}{2}m. \end{cases}$$

Moreover, the preperiod of this sequence has length less than $2m+1$.

Proof. Indeed, for $k_1, k_2 \ge 2m+1$, we have

$$\begin{aligned} y_{2k_1} - y_{2k_2} &\equiv (k_1 - k_2)(1 - a^{-1}y_0^2)b - (k_1 - k_2)(k_1 + k_2 + 1)a^{-1}b^2y_0 + \\ &+ (k_1 - k_2)a^{-1}cy_0^{-1}(a^2 - y_0^4) + p^\alpha(F_0(k_1) - F_0(k_2)) \pmod{p^m} \end{aligned} \tag{11}$$

Hence, $y_{2k_1} - y_{2k_2} = A(k_1 - k_2)p^\nu$, where $(A, p) = 1$, and thus $y_{2k_1} - y_{2k_2} \equiv 0 \pmod{p^m}$ if and only if $k_1 - k_2 \equiv 0 \pmod{p^{m-\nu}}$. □

Corollary 2.3. *Let $p = 2$, $m \ge 3$, $b = 2^\nu b_0$, $(b_0, 2) = 1$, $c = 2^\mu c_0$, $(c_0, p) = 1$, $\mu > \nu > 0$; $\nu_p(a - y_0^2) = \nu_0 \ge 1$. Then the sequence $\{y_n\}$ defined by recursion (2) is purely periodic with period*

$$\tau = \begin{cases} 2^{m-2\nu+1} & \text{if } m \ge 2\nu,\ \nu_0 > \nu; \\ 2^{m-2\nu-\beta_0+1} & \text{if } m > 2\nu,\ \nu_0 = \nu,\ \beta_0 = \nu_p\left(\frac{y_0^2 - a}{2^{\nu_0}} + b_0\right); \\ 2^{m-\nu-\nu_0+1} & \text{if } m \ge \nu + nu_0,\ \nu_0 < \nu. \end{cases}$$

Proof. This follows from the relation (11) which holds for $p = 2$. □

Remark 2.4. From the first two cases for τ in Corollary 2.3 we obtain that for $\nu_0 \ge \nu$ the maximal period $\tau = 2^{m-2\nu+1}$ achieves if and only if $\nu_0 > \nu$ and $m \ge 2\nu$. In [10] this assertion was obtained for $\nu = 1$.

3. Discrepancy bound

Equidistribution and statistical independence properties of pseudorandom numbers can be analyzed using the discrepancy of certain sequences of points in $[0,1)^s$.

For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0,1)^s$, the discrepancy is defined by

$$D_N^{(s)}(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) := \sup_I \left| \frac{A_N(I)}{N} - |I| \right|,$$

where the supremum is taken over all subintervals I of $[0,1)^s$, $A_N(I)$ is the number of points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into I, and $|I|$ denotes the s-dimensional volume I.

Beside discrepancy there exist other important criteria for the uniformity and the independence of PRN's. We shall restrict our attention to the discrepancy, since it is the most important measure of uniformity and independence related to PRN's. For upper estimate of the discrepancy of points we will use the following inequality from [13, Th. 3.10, p.34].

Lemma 3.1. *Let $q > 1$ and s be natural numbers and let $\{Y_n\}$, $Y_n \in \{0, 1, \ldots, q-1\}^s$, be a purely periodic sequence with a period τ. Then the points $X_n = \frac{Y_n}{q} \in [0,1)^s$, $n \in \{0, 1, \ldots, N-1\}$, $N \le \tau$, have discrepancy*

$$D_N^{(s)}(X_0, X_1, \ldots, X_{N-1}) \le \frac{s}{q} + \frac{1}{N} \sum_{h_0, h_1, \ldots, h_s} \frac{1}{\overline{h}_0 \overline{h}_1 \cdots \overline{h}_s} |S|, \tag{12}$$

where the summation runs over all integers $h_0, h_1, \ldots, h_s$ for which $h_0 \in \left(-\frac{\tau}{2}, \frac{\tau}{2}\right]$, $h_i \in \left(-\frac{q}{2}, \frac{q}{2}\right]$, $(i = 1, \ldots, s)$, $(h_1, \ldots, h_s) \ne (0, \ldots, 0)$, $\overline{h}_i = \max(1, |h_i|)$, and

$$S := \sum_{n=0}^{\tau-1} e\Big(h \cdot X_n + \frac{n h_0}{\tau}\Big),$$

where $h \cdot X_n = \sum\limits_{i=1}^{s} h_i x_i^{(n)}$ stands for the inner product of h and X_n in $\mathbb{Z}^s$.

The following lemma is a special version of Niederreiter's result [13, Th. 3.10, p. 34; Cor. 3.17, p. 43].

Lemma 3.2. *The discrepancy of N arbitrary points $\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}} \in [0,1)^2$ satisfies*

$$D_N^{(2)}(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) \ge \frac{1}{2(\pi+2)\,|h_1 h_2|\, N} \cdot \Big| \sum_{k=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_k}) \Big| \tag{13}$$

for any lattice point $\mathbf{h} = (h_1, h_2) \in \mathbb{Z}^2$ with $h_1 h_2 \ne 0$.

For applications of Lemmas 3.1 and 3.2 we shall need the following estimates of exponential sums of sequences of pseudorandom numbers, which can be proved by analogy with Theorems 1 and 2 in [16].

Theorem 3.3. *Let $(h_1, h_2, p) = 1$, $\nu_p(h_1 + h_2) = \beta$, $\nu_p(h_1 k + h_2 \ell) = \gamma$, $k, \ell \geq 0$. For the sequence $\{y_n\}$ produced by (2) we get*

$$|\sigma_{k,\ell}(h_1, h_2; p^m)| \leq \begin{cases} (2p)^{\frac{m}{2}} & \text{if } k \not\equiv \ell \pmod 2; \\ 0 & \text{if } k \equiv \ell \pmod 2 \text{ and } \beta < \gamma + \nu,\ m - \beta - \nu > 0; \\ p^{m-1}(p-1) & \text{if } k \equiv \ell \pmod 2 \text{ and } \beta \geq \gamma + \nu,\ m - \nu - \gamma \leq 0; \\ 2p^{\frac{m+\nu+\gamma}{2}} & \text{if } k \equiv \ell \pmod 2 \text{ and } \beta \geq \gamma + \nu,\ m - \nu - \gamma > 0. \end{cases}$$

Let τ be the least length of a period of the sequence $\{y_n\}$.

Theorem 3.4. *Let the linear-inversive congruential sequence generated by the recursion (2) has period τ, and let $\nu_p(b) = \nu$, $\nu_p(a - y_0^2) = \nu_0$, $\nu_p(h) = s$, $2\nu \leq m$. Then*

$$|S_\tau(h, y_0)| \leq \begin{cases} O(m) & \text{if } p > 2 \text{ and } \nu_0 < \nu,\ s < m - \nu - \nu_0, \\ & \text{or } p = 2 \text{ and } \nu_0 < \nu,\ \nu_2(h) < m - 2\nu; \\ 4 \cdot 2^{\frac{m+s}{2}} & \text{if } \nu_0 \geq \nu,\ s < m - 2\nu; \\ \tau & \text{otherwise.} \end{cases}$$

Let $\{y_n\}$ be a sequence of PRN's generated by (2) and let $x_n = \frac{y_n}{p^m}$, $n \geq 0$. The sequence $\{x_n\}$ induces a sequence $\{X_n^{(s)}\}$ of vectors in $[0, 1)^s$ defined by $X_n^{(s)} := (x_n, x_{n+1}, \ldots, x_{n+s-1})$. We shall say that the sequence $\{x_n\}$ passes d-dimensional serial test on unpredictability (statistical independency) if for every $s \leq d$ the sequence $\{X_n^{(s)}\}$ has uniform distribution.

Theorem 3.5. *Let $p > 2$ be a prime number and m, a, b, c, y_0 be integers, $m \geq 3$, $(y_0, p) = (a, p)$, $0 < \nu_p(b) < \nu_p(c)$, $a \not\equiv y_0^2 \pmod p$. Then for $m \geq 2\nu$ and for the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$, where y_n defined by the recursion (2), we have*

$$D_N^{(1)}(x_0, x_1, \ldots, x_{N-1}) \leq 3N^{-1} p^{\frac{m}{2}} \log^2 p^m. \tag{14}$$

Proof. By $a \not\equiv y_0^2 \pmod p$ we have $\tau = p^{m-\nu}$. From Lemma 3.1 (for $s = 1$, $q = p^m$) we get

$$D_N^{(1)}(x_0, x_1, \ldots, x_{N-1}) \leq \frac{1}{p^m} + \frac{1}{N} \sum_{0<|h|<\frac{1}{2}p^m} \sum_{h_0 \in \left(-\frac{\tau}{2}, \frac{\tau}{2}\right]} \frac{1}{\overline{h} \cdot \overline{h}_0} \left| \sum_{n=0}^{\tau-1} e^{2\pi i \left(\frac{h y_n}{p^m} + \frac{n h_0}{\tau}\right)} \right| \leq$$

$$\frac{1}{p^m} + \frac{1}{N} \sum_{h, h_0} \frac{1}{\overline{h} \cdot \overline{h}_0} \left(\left| \sum_{k=0}^{p^{m-\nu}-1} e\Big(\frac{h y_{2k}}{p^m} + \frac{k h_0}{p^{m-\nu}}\Big) \right| + \left| \sum_{k=0}^{p^{m-\nu}-1} e\Big(\frac{h y_{2k+1}}{p^m} + \frac{(2k+1) h_0}{p^{m-\nu}}\Big) \right| \right). \tag{15}$$

By (10) the estimates of two last sum can be obtained.
We have

$$\sum\nolimits_1 := \sum_{k=0}^{p^{m-\nu}-1} e\Big(\frac{h y_{2k}}{p^m} + \frac{k h_0}{p^{m-\nu}}\Big) = \sum_{k=0}^{p^{m-\nu}-1} e\Big(\frac{\overline{A}_1 k + \overline{A}_2 k^2 + p^{\alpha_1} h F(k)}{p^{m-\nu}}\Big),$$

where

$$\overline{A}_1 = h b_0 (1 - a^{-1} y_0^2) + h c_0 p^{\mu-\nu} (1 - a^{-2} y_0^4) + h_0 + h a^{-1} b_0^2 p^\nu y_0,$$
$$\overline{A}_2 = h a^{-1} b_0^2 p^\nu, \qquad \alpha_1 = \alpha - \nu = \min(2\nu, \mu).$$

Using Lemma 1.2, we infer that $|\sum_1| \le 2p^{\frac{m}{2}}$ for $m \ge 2\nu$. An analogous estimate can be deduced for the sum $\sum_2$. Hence,

$$D_N^{(1)}(x_0, x_1, \ldots, x_{N-1}) \le \frac{1}{p^m} + N^{-1} \cdot 2p^{\frac{m}{2}} \log^2 p^m \le 3N^{-1} p^{\frac{m}{2}} \log^2 p^m.$$

□

Remark 3.6. If the period $\tau < 2p^{m-\nu}$ (i.e., $\nu_p(1 - a^{-1}y_0^2) > 0$), then the sums $\sum_1$ and $\sum_2$ may be uncomplete, and thereby we have bound $D_N(x_0, x_1, \ldots, x_{N-1}) \le 3N^{-1}p^{\frac{m}{2}} \log^3 p^m$.

Remark 3.7. In the case $p = 2$ we obtain easily that for the maximal period $\tau = 2^{m-1}$, $D_N(x_0, x_1, \ldots, x_{N-1}) \le 3N^{-1}2^{\frac{m}{2}} \log^2 2^m$.

Theorem 3.8. *For points constructed by the linear-inversive congruential generator (2) with parameters a, b, c satisfying the condition*

$$0 < \nu_p(b) = \nu,\ 2\nu < \mu = \nu_p(c),\ a \not\equiv y_0^2 \pmod p,$$

the discrepancy $D_N^{(s)}$, $s \in \{2, 3, 4\}$, has an upper bound

$$D_\tau^{(s)} \le \frac{s}{2p^{m-\nu}} + p^{-\frac{m-2\nu}{2}} \log^s p^m. \tag{16}$$

Proof. Consider only the case $s = 4$ (cases $s = 2$ and $s = 3$ can be considered similarly). In order to apply Lemma 3.1 we must have an estimate for the sum

$$\sum_{n=0}^{\tau-1} e\Big(\frac{h_1 y_n + h_2 y_{n+1} + h_3 y_{n+2} + h_4 y_{n+3}}{p^m}\Big).$$

Without loss of generality, we can suppose that $(h_1, h_2, h_3, h_4, p) = 1$. Using (10) we can write

$$y_{2k} = A_0 + A_1 k + A_2 k^2 + A_3 k^3 := f(k), \quad y_{2k+1} = B_0 + B_1 k + B_2 k^2 + B_3 k^3 := g(k),$$

where modulo p^α

$$\begin{aligned}
A_0 &= A_0(y_0) \equiv y_0 \\
A_1 &= A_1(y_0) \equiv b(1 - a^{-1}y_0^2) + a^{-1}b^2 y_0 + acy_0^{-1}(1 - a^{-2}y^4) \\
A_2 &= A_2(y_0) \equiv -a^{-1}b^2 y_0 + a^{-2}b^2 y_0^3 = -a^{-1}b^2 y_0(1 - a^{-1}y_0^2) \\
B_0 &= B_0(y_0) \equiv b + ay_0^{-1} + cy_0 \\
B_1 &= B_1(y_0) \equiv b(1 - ay_0^{-2}) - b^2 y_0^{-1} - y_0 c(1 - a^2 y_0^{-4}) \\
B_2 &= B_2(y_0) \equiv -b^2 y_0^{-1} + ab^2 y_0^{-3} = -b^2 y_0^{-1}(1 - ay_0^{-2}) \\
A_3 &= A_3(y_0, k) \equiv B_3(y_0, k) \equiv B_3 \equiv 0.
\end{aligned} \tag{17}$$

Hence,

$$h_1 y_{2k} + \cdots + h_4 y_{2k+3} = C_0 + C_1 k + C_2 k^2 + p^\alpha L(h_1, h_2, h_3, h_4, k).$$

Using (17) we can write

$$C_1 := C_1(h_1, h_2, h_3, h_4) = (h_1 + h_3)A_1 + (h_2 + h_4)B_1 + 2A_2h_3 + 4B_2h_4,$$
$$C_2 := C_2(h_1, h_2, h_3, h_4) = (h_1 + h_3)A_2 + (h_2 + h_4)B_2.$$

Since $1 - a^{-1}y_0^2 \not\equiv 0 \pmod p$, the congruences

$$C_1 \equiv 0 \pmod{p^{2\nu+1}} \text{ and } C_2 \equiv 0 \pmod{p^{2\nu+1}}$$

cannot hold simultaneously. Then Lemma 1.2 implies

$$\left|\sum\nolimits_1\right| \le \begin{cases} 2p^{\frac{m+\nu}{2}} & \text{if } C_1(h_1, h_2, h_3, h_4) \equiv 0 \pmod{p^{2\nu}}, \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

Similarly, we have

$$\left|\sum\nolimits_2\right| \le \begin{cases} 2p^{\frac{m+\nu}{2}} & \text{if } D_1(h_1, h_2, h_3, h_4) \equiv 0 \pmod{p^{2\nu}}, \\ 0 & \text{otherwise,} \end{cases} \tag{19}$$

where $D_1(h_1, h_2, h_3, h_4)$ are defined (similarly to $C_1(h_1, h_2, h_3, h_4)$) by the representation

$$h_1y_{2k+1} + h_2y_{2k+2} + h_3y_{2k+3} + h_4y_{2k+4} = D_0 + D_1k + D_2k^2 + D_3k^3 + p^\alpha M(h_1, h_2, h_3, h_4, k).$$

Here the functions $L(h_1, h_2, h_3, h_4, k)$ and $M(h_1, h_2, h_3, h_4, k)$ are polynomials of its variables over $\mathbb{Z}$.

Now, Lemma 3.1 and simple calculations give $D_\tau^{(4)} \le \frac{4}{2p^{m-\nu}} + p^{-\frac{m-2\nu}{2}} \log^4 p^m$. $\square$

Theorem 3.9. *Let p be a prime and m, a, b, c and y be integers with $m \ge 3$. Suppose that $(a, p) = 1$, $b \equiv c \equiv 0 \pmod p$, $bc \equiv 0 \pmod{p^m}$, $b^2 \not\equiv 0 \pmod{p^m}$, $\nu_p(b) < \nu_p(c)$, and $a^2 \not\equiv y^4 \pmod p$. Then for the sequence $\mathbf{t_k} = (x_k, x_{k+1})$, $k \ge 0$, where $x_k = \frac{y_k}{p^m}$, y_k are defined by the recursion (2) we have*

$$D_\tau^{(2)}(\mathbf{t_0}, \ldots, \mathbf{t_{\tau-1}}) \ge \frac{1}{4(\pi + 2)h^*} p^{-(\frac{m}{2}-\nu)}, \tag{20}$$

where $\nu = \nu_p(b)$, $h^* = \min\{|h_1h_2| : h_1 \equiv h_2ay^{-2} \pmod{p^\nu},\ (h_1, p) = 1\}$.

This theorem can be proved in the same way as Theorem 9 from [15].

Theorems 3.8 and 3.9 show that, in general, the upper bound is the best possible up to the logarithmic factor for any sequence $\{x_n, x_{n+1}, \ldots, x_{n+s-1}\}$, $k \ge 0$ (defined by the recursion (2) since there exist a sequence $\{x_n, x_{n+1}, \ldots, x_{n+s-1}\}$ with $D_\tau^{(s)} \ge \frac{1}{8(\pi+2)} p^{-(\frac{n}{2}-\nu)}$.

Hence, on the average the discrepancy $D_\tau^{(2)}$ has an order of magnitude between $p^{-(\frac{n}{2}-\nu)}$ and $p^{-(\frac{n}{2}-\nu)} \log^2 p^n$. In certain sense, the sequence generated by (2) models the random numbers very closely.

REFERENCES

1. S.R. Blackburn, D. Gomez-Peres, J. Gutierrez, I. Shparlinski, *Predicting nonlinear pseudorandom number generators*, Math. Comp. **74**:251 (2005), 1471–1494.

2. S.R. Blackburn, D. Gomez-Peres, J. Gutierrez, I. Shparlinski, *Reconstructing noisy polynomial evaluation in residue rings*, J. Algorithm, **61**:2 (2006), 47–59.

3. J. Eichenauer-Herrmann, F. Emmerich, *Compound inversive congruential pseudorandom numbers: an average-case analysis*, Math. Comp. **65**:213 (1996), 215–225.

4. J. Eichenauer-Herrmann, H. Grothe, *A new inversive congruential pseudorandom number generator with power of two modulus*, ACM Transactions of Modeling and Computer Simulation. **2**:1 (1992), 1–11.

5. J. Eichenauer-Herrmann, E. Herrmann, S. Wegenkittl, *A survey of quadratic and inversive congruential pseudorandom numbers*, in: Monte Carlo and Quasi-Monte Carlo Methods, 1996, H. Niederreiter et al(eds.), Lecture Notes in Statist. **127**, Springer, New York, (1998), 66–97.

6. J. Eichenauer, J. Lehn, *A non-linear congruential pseudo random number generator*, Statist. Papers **27**:1 (1986), 315–326.

7. J. Eichenauer, J. Lehn, A. Topuzoğlu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51**:184 (1988), 757–759.

8. M. Flahive, H. Niederreiter, *On inversive congruential generators for pseudorandom numbers*, G.L. Mullen, P.J.-S. Shiue (Eds.), Finite Fields, Coding Theory, and Advances in Communications and Computing, Dekker, New York.(1992), 75–80.

9. N. M. Korobov, *Exponential sums and its applications*, M.: Nauka, (1989), 240 p.

10. T. Kato, L.-M. Wu, N. Yanagihara, *On a nonlinear congruential pseudorandom number generator*, Math. Comput. **65**:213 (1996), 227–233.

11. H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Advances in Math. **26**:2 (1977), 99–181.

12. H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84**:6 (1978), 957–1041.

13. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conference Series in Applied Mathematics, SIAM, Philadelphia, (1992), 243 p.

14. H. Niederreiter, I. Shparlinski, *Recent advances in the theory of nonlinear pseudorandom number generators*, Monte Carlo and Quasi-Monte Carlo Methods (2000), Springer, Berlin. (2002), 86–102.

15. P. Varbanets, S. Varbanets, *Exponential sums on the sequences of inversive congruential pseudorandom numbers with prime-power modulus*, VoronoÏ's Impact on modern science, Proceedings of the 4th International Conference on Analytic Number Theory and Spatial Tessellations, Book 4, Volume 1, Kyiv, Ukraine. (September 22-28, 2008), 112–130.

16. P. Varbanets, S. Varbanets, *Generalizations of inversive congruential generator*, Analytic and probabilistic methods in number theory, TEV, Vilnius, (2012), 265–282.

Received 13.11.2012

Revised 03.09.2013