Annales Univ. Sci. Budapest., Sect. Comp. 48 (2018) 225–232

EXPONENTIAL SUMS OVER THE SEQUENCES OF PRN'S PRODUCED BY INVERSIVE GENERATORS

Sergey Varbanets (Odessa, Ukraine)

Communicated by Imre Kátai

(Received February 20, 2018; accepted March 10, 2018)

Abstract. The inversive congruential method for generating uniform pseudorandom numbers is a particulary attractive alternative to linear congruential generators, which show many undesirable regularities. Exponential sums on inversive congruential pseudorandom numbers are estimates.

1. Introduction

The character of equidistribution the sequence of pseudorandom numbers (abbreviate, PRN's) is defined by the discrepancy of this sequence. Usually the bound of discrepancy for the sequence of PRN's, that is generated by the congruential generator, is estimated by using the Turán–Erdős–Koksma inequality, the core of which is the exponential sum with elements of this sequence in exponent.

In the works of R.G. Stoneham [5] and H. Niederreiter [2]–[4] a certain exponential sums are investigated which are intimately connected with the linear congruential PRN's produced by the linear congruential recursion

$$y_{n+1} \equiv ay_n + b \pmod{M},\ n = 0, 1, 2, \ldots,\ (0 \leq y_1 \leq M),$$

where $a, b, M, y_0 \in \mathbb{Z}$, $a \geq 1$, $M > 1$, $b, y_0 \geq 0$.

Key words and phrases: Inversive congruential pseudorandom numbers, exponential sum, equidistribution.

2010 Mathematics Subject Classification: Primary 11L07; Secondary 45B67, 11T23, 11T71, 11K45.

H. Niederreiter [4] proved the following assertion

Theorem. *Let $h \in \mathbb{Z}$, $(h, M) = 1$, $(a, M) = 1$, and assume that a belongs to the exponent ℓ modulo M. Then, for $1 \le N \le \tau$*

$$\left|\sum_{n=0}^{N-1} e^{2\pi i \frac{hy_n}{M}}\right| < \left(\frac{M\tau}{\ell}\right)^{\frac{1}{2}} \left(\frac{2}{\pi}\log\tau + \frac{3}{4}\right),$$

where τ is the least period length of the sequence $\{y_n\}$.

The well-known deficiencies of the linear congruential sequences of PRN's, such as the relatively coarse lattice structure of these sequences, and as consequence a predictability of elements of the linear congruential generators of PRN's.

Let $f(x)$ be an integral-value function and let $\{y_n\}$ be a sequence produced by the congruential recursion

$$y_{n+1} \equiv f(y_n) \pmod{M}$$

with initial value y_0.

Consider the sequence $\{x_n\}$, $x_n = \dfrac{y_n}{M}$, $n = 0, 1, \ldots$. This sequence calls the sequence of PRN's if it is an equidistribution on $[0, 1)$, statistical independence and has "a large" period length.

In 1986 Eichenauer and Lehn [1] and then Niederreiter [2] have studied a recursive sequence generated by the recursive relation

$$y_{n+1} \equiv \begin{cases} ay_n^{-1} + b \pmod{p}, & \text{if } (y_n, p) = 1 \\ b \pmod{b}, & \text{if } y_n \equiv 0 \pmod{p} \end{cases}$$

with some coefficients $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}_p$, $(y_0, p) = 1$, y_n^{-1} is a multiplicative inverse for y_n modulo p.

Such generator of PRN's calls the inversive generator modulo p. For the case $M = p^m$, $m > 1$, we also can consider similar generator if only for all $n = 0, 1, 2, \ldots$ the values y_n satisfy the condition $(y_n, p) = 1$. This condition holds if $(a, p) = 1$, $b \equiv 0 \pmod{p}$.

In the sequel we shall always assume also without of explicit mention that this condition accomplishes.

In the present paper we study some exponential sums over the sequence of inversive congruential PRN's $\{y_n\}$ produced by one congruence

$$\text{(I)} \quad y_{n+1} \equiv ay_n^{-1} + b(n) \pmod{p^m},$$

$$\text{(II)} \quad y_{n+1} \equiv ay_{n-1}^{-1}y_n^{-1} + b(n) \pmod{p^m},$$

where $b(n) = b + c_1 n + p^{\mu} F(n)$, $b = p^{\nu_0} b_0$, $\nu_0 > 0$, $(b_0, p) = 1$, $c_1 = c y_0$, $\nu_p(c) = \mu_0 > \nu_0$ (for (I)), and $c_1 = c$ (for (II)); $(a, p) = (y_0, p) = (y_1, p) = 1$, $\mu > \max(\nu_0, \mu_0)$, $F(n) \in \mathbb{Z}[n]$.

The generator of PRN's (I) (respectively, (II)) calls the inversive generator with a variable shift (respectively, the inversive generator of second order with a variable shift).

The aim of this paper to obtain non-trivial bounds for the exponential sums of type

$$S_\ell^{(j)}(h; N) = \sum_{\substack{n=0 \\ y_n \in (\ell)}}^{N-1} e^{2\pi i \frac{h y_n^j}{p^m}}, \quad j = 1,\, 2;\ \ell = \mathrm{I},\, \mathrm{II};$$

$$K_\ell(h_1, h_2; N) = \sum_{\substack{n=0 \\ y_n \in (\ell)}}^{N-1} e^{2\pi i \frac{h_1 y_n + h_2 y_n^{-1}}{p^m}}, \quad \ell = \mathrm{I},\, \mathrm{II}.$$

Here we note that the subscription $y_n \in (\ell)$ implies the satisfaction of y_n to recursion (ℓ) ($\ell = \mathrm{I}$ or II).

Notations. The letter p denotes a prime number, $p \geq 5$. For $m \in \mathbb{N}$, the notation $\mathbb{Z}_M$ (respectively, $\mathbb{Z}_M^*$) denotes the complete (respectively, reduced) system of residue modulo M. We write $gcd(a, b) = (a, b)$ for the greatest common divisor of a and b. For $z \in \mathbb{Z}$, $(z, p) = 1$, let z^{-1} be the multiplicative inverse modulo p^m. Through $\nu_p(A)$ we denote the p-adic valuation of $|A| \in \mathbb{Z}_{>0}$, throughout the sequel, for brevity, we write $e_q(n) = e^{2\pi i \frac{n}{q}}$ for integer n.

2. Auxiliary results

Now we consider some lemmas which will be necessary furthermore.

Lemma 1 (see, [7]). *Let $\{y_n\}$ be the sequence produced by recursion* (I) *under its conditions. Then for $k > \left[\frac{m}{\nu_0}\right] + 1$ the following representations modulo p^m*

$$\begin{cases} y_{2k} = \dfrac{A_0^{(k)} + A_1^{(k)} y_0 + \cdots + A_{r-1}^{(k)} y_0^{r-1}}{B_0^{(k)} + B_1^{(k)} y_0 + \cdots + B_r^{(k)} y_0^r}, \\[2ex] y_{2k+1} = \dfrac{C_0^{(k)} + C_1^{(k)} y_0 + \cdots + C_r^{(k)} y_0^r}{D_0^{(k)} + D_1^{(k)} y_0 + \cdots + D_{r-1}^{(k)} y_0^{r-1}} \end{cases}$$

hold.

Moreover, we have

$$\begin{aligned}
A_j^{(k)} &= aD_j^{(k)} + bC_j^{(k)} + F(2k+2)C_{j-1}^{(k)},\ j = 0,1,\ldots,r-1;\\
A_r^{(k)} &= bC_r^{(k)};\\
B_j^{(k+1)} &= C_j^{(k)},\ j = 0,1,\ldots,r;\\
C_j^{(k+1)} &= aB_j^{(k+1)} + bA_j^{(k+1)} + F(2k+3)A_j^{(k+1)},\ j = 0,1,\ldots,r-1;\\
C_r^{(k+1)} &= bA_r^{(k+1)},\ D_j^{(k+1)} = A_j^{(k+1)},\ j = 0,1,\ldots,r-1;\\
F(u) &= c(u + p^{\mu}F_0(u)),\ c = c_1 y_0^{-1}.
\end{aligned}$$

Corollary. *For all $k \geq 2$ we have modulo p^{ν}*

$$y_{2k} = \frac{kb + \left(1 + a^{-1}\,\frac{k(k+1)}{2}\,b^2 + k(k+1)c\right) y_0}{\left(1 + \frac{k(k+1)}{2}\,a^{-1}\,b^2\right) + ka^{-1}b^2y_0 + (2k-1)a^{k-1}cy_0^2},$$

$$y_{2k+1} = \frac{\left(a^{k+1} + \frac{k(k+1)}{2}\,a^k\,b^2 + (k+1)a^kb^2y_0 + (2k+1)a^kcy_0^2\right)}{ka^kb + \left(a^k + \frac{k(k+1)}{2}\,a^{k-1}b^2 + a^k + k(k+1)c\right) y_0}$$

Lemma 2 (see, [6])**.** *Let y_n be produced by inversive generator of type (II). Then the following representations*

$$y_{3k-1} = \frac{a^k + c^{k-1}\,b^2\,\frac{k(k-1)}{2}\,y_0 + \left(a^{k-1}bk + a^{k-1}c\Phi_1(k)\right) y_0y_1}{\left(\frac{k(k-1)}{2}\,a^{k-1}b^2 + a^{k-1}c\Phi_2(k)\right) + (k-1)a^{k-1}by_0 + a^{k-1}y_0y_1},$$

$$y_{3k} = \frac{ka^kb + a^ky_0 + \left(\frac{k(k-1)}{2}\,a^{k-1}b^2 + a^{k-1}c\Phi_3(k)\right) y_0y_1}{a^k + \frac{k(k-1)}{2}\,a^{k-1}b^2y_0 + (ka^{k-1}b + a^{k-1}c\Phi_1(k))\,y_0y_1},$$

$$y_{3k+1} = \frac{\left(\frac{k(k-1)}{2}\,a^kb^2 + a^kc\Phi_2(k+1)\right) + ka^2by_0 - a^ky_0y_1}{ka^kb + a^ky_0 + \left(\frac{k(k-1)}{2}\,a^{k-1}b^2 + a^{k-1}c\Phi_3(k)\right) y_0y_1},$$

hold, where

$$\begin{aligned}
&\Phi_1(k) = F_2 + F_5 + \cdots + F_{3k-1},\\
&\Phi_2(k) = F_4 + F_7 + \cdots + F_{3k-2},\\
&\Phi_3(k) = F_3 + F_6 + \cdots + F_{3k},\\
&F_j = j + p^{\mu_1}F_1(j),\ \ F_1(n) \in \mathbb{Z}[n],\ \mu_1 \geq 1.
\end{aligned}$$

Lemma 3 (see, [6], Lemma 2)**.** *Let h_1, h_2, k, ℓ be positive integers and let $\nu_p(h_1+h_2)=\alpha$, $\nu_p(h_1k+h_2\ell)=\beta$, $\delta=\min(\alpha,\beta)$. Then for every $j=2,3,\dots$ we have*

$$\nu_p(h_1k^{j-1}+h_2\ell^{j-1})\geq\delta.$$

Moreover, for every polynomial $G(u)=A_1u+A_2u^2+p^tG_1(u)\in\mathbb{Z}[u]$ we have

$$h_1G(k)+h_2G(\ell)=A_1(h_1k+h_2\ell)+A_2(h_1k^2+h_2\ell^2)+p^{t+s}G_2(k,\ell),$$

where $s\geq\min(\nu_p(h_1+h_2),\nu_p(h_1k+h_2\ell))$, $h_1,h_2,k,\ell\in\mathbb{Z}$, $G_2(u,v)\in\mathbb{Z}[u,v]$.

Lemma 4 (see, [6], Lemma 3)**.** *Let $p>2$ be a prime number, $m\geq 2$ be a positive integer, $m_0=\left[\frac{m}{2}\right]$, $f(x)$, $g(x)$, $h(x)$ be polynomials over $\mathbb{Z}$*

$$\begin{aligned}f(x)&=A_1x+A_2x^2+\cdots,\\ g(x)&=B_1x+B_2x^2+\cdots,\\ h(x)&=C_\ell x+C_{\ell+1}x^{\ell+1}+\cdots,\ \ell\geq 1,\end{aligned}$$

$$\nu_p(A_j)=\lambda_j,\quad \nu_p(B_j)=\mu_j,\quad \nu_p(C_j)=\nu_j,$$

and moreover,

$$\begin{aligned}&k=\lambda_2<\lambda_3\leq\cdots,\quad 0=\mu_1<\mu_2<\mu_3\leq\cdots,\\ &\nu_p(C_\ell)=0,\ \nu_p(C_j)>0,\ j\geq\ell+1.\end{aligned}$$

Then the following bounds occur

$$\left|\sum_{x\in\mathbb{Z}_{p^m}}e_m(f(x))\right|\leq\begin{cases}2p^{\frac{m+k}{2}} & if\quad \nu_p(A_1)\geq k,\\ 0 & if\quad \nu_p(A_1)<k;\end{cases}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}}e_m(f(x)+g(x^{-1}))\right|\leq I(p^{m-m_0})p^{\frac{m}{2}}$$

$$\left|\sum_{x\in\mathbb{Z}^*_{p^m}}e_m(h(x))\right|\leq\begin{cases}1 & if\quad \ell=1,\\ 0 & if\quad \ell>1,\end{cases}$$

where $I(p^{m-m_0})$ is a number of solutions of the congruence

$$y\cdot f'(y)\equiv g'(y^{-1})\cdot y^{-1}\pmod{p^{m-m_0}},\ y\in\mathbb{Z}^*_{p^{m-m_0}}.$$

3. Main results

For the sequence type (I) by Lemma 1 we have

Lemma 5. *Let $\{y_n\}$ be the sequence produced by recursion* (I) *under its conditions. Then for $k \geq 2$ there are valid the following representations modulo p^ν*

$$\begin{aligned} y_{2k} = {} & y_0\left(1-a^{-1}y_0^2\right)+k\left(b\left(1-a^{-1}y_0^2\right)+(2a)^{-1}b^2y_0+cy_0\right)+ \\ & +k^2\left(-a^{-1}y_0\left(1-a^{-1}y_0^2\right)b^2+a^{-1}cy_0^2\right):=E_0+E_1k+E_2k^2; \end{aligned}$$

$$\begin{aligned} y_{2k+1} = {} & \left(ay_0^{-1}+b+cy_0\right)+k\left(b\left(1-ay_0^{-2}\right)+b^2+2cy_0\right)+ \\ & +k^2\left(-\left(1-ay_0^{-2}\right)b^2-\frac{1}{2}(4-a^{-1})b^2y_0^{-1}-ac\right):=F_0+F_1k+F_2k^2; \end{aligned}$$

From here the following assertion follows immediately:

Corollary. *The period length τ of the sequence $\{y_n\}$ is equal to $2p^{m-\nu_0}$ if a is a quadratic non-residue modulo p. And hence, the maximal period length takes out for $\nu_p(b)=\nu_0=1$.*

For the sequence type (II) by Lemma 2 we have

Lemma 6. *Let $\{y_n\}$ be the sequence produced by recursion (II) under its conditions. Then for $k \geq 2$ the following representations modulo p^ν*

$$\begin{aligned} y_{3k-1} = {} & ay_0^{-1}y_1^{-1}+(k-1)b\left(\left(-ay_0^{-2}y_1^{-1}+1\right)-\frac{1}{2}by_1^{-1}\left(ay_0^{-2}y_1^{-1}-1\right)\right)+ \\ & +(k-1)^2b^2\frac{1}{2}y_0^{-1}\left(-1+a^{-1}y_0y_1^2\right), \end{aligned}$$

$$\begin{aligned} y_{3k} = {} & \left(y_0+a^{-1}by_0^2y_1+b^2y_0^3y_1^2+a^{-1}b^2y_0y_1\right)+ \\ & +k\left(b+a^{-1}b^2y_0y_1-\frac{1}{2}a^{-1}b^2y_0^2-\right. \\ & \left.-a^{-1}by_0^2y_1-2b^2y_0^3y_1^2-\frac{1}{2}a^{-1}b^2y_0y_1\right)+ \\ & +k^2\left(-a^{-1}b^2y_0y_1-\frac{1}{2}a^{-1}b^2y_0^2+b^2y_0^3y_1^2+\frac{1}{2}a^{-1}b^2y_0y_1\right), \end{aligned}$$

$$\begin{aligned} y_{3k+1} = {} & \left(y_1-a^{-1}b^2y_1^2\right)+kb\left(\frac{1}{2}b\left(y_0^{-1}-a^{-1}y_1^2\right)+1-y_0^{-1}y_1\right)+ \\ & +k^2b^2\frac{1}{2}\left(-y_0^{-1}+a^{-1}b^2y_1^2\right) \end{aligned}$$

hold.

Corollary. *If at least one of the congruences*

$$a \equiv y_0^2 y_1 \pmod{p^{\nu_0}}, \quad a \equiv y_0 y_1^2 \pmod{p^{\nu_0}}$$

is violated then the sequence (II) *has a period length* τ *equal to* $3p^{m-\nu_0}$. *If* a *is a cubic non-residue modulo* p *and* $y = y_0 \pmod{p^\nu}$ *we have the same period length. And hence, the maximal period length takes out for* $\nu_p(b) = \nu_0 = 1$.

Now, from representations $\{y_n\}$ obtained above for the sequences (I) and (II) we infer (by Lemma 4)

Theorem 1. *Let* $\{y_n\}$ *be the sequence of PRN's produced by recursion* (ℓ), $\ell = \mathrm{I},\ \mathrm{II}$, *where* a *is a quadratic non-residue modulo* p. *Then*

$$S_\ell^{(j)}(h;N) = \sum_{\substack{n=0 \\ y_n \in (\ell)}}^{N-1} e^{2\pi i \frac{h y_n^j}{p^m}} \ll p^{\frac{m+\nu_0}{2}}, \ j \in \mathbb{Z},\ (j,p)=1,\ (h,p)=1$$

hold.

Theorem 2. *Let* h_1, h_2 *be arbitrary integers with* $s = \nu_p(gcd(h_1, h_2, p^m))$, $s \le m - \nu_0$. *Then for the sequence* $\{y_n\}$ *produced by recursion* (ℓ), $\ell = \mathrm{I},\ \mathrm{II}$ *and with a maximal period length* $\tau = 3p^{m-\nu_0}$ *we have*

$$K_\ell(h_1,h_2;N) = \sum_{\substack{n=0 \\ y_n \in (\ell)}}^{N-1} e^{2\pi i \frac{h_1 y_n + h_2 y_n^{-1}}{p^m}} \ll p^{\frac{m+\nu_0+s}{2}}.$$

To prove the estimates for above sums it is enough to split the summation over n for two parts $n \equiv 0 \pmod 2$ and $n \equiv 1 \pmod 2$ for $\ell = \mathrm{I}$ and, respectively, for three parts $n \equiv -1 \pmod 3$, $n \equiv 0 \pmod 3$ and $n \equiv 1 \pmod 3$ for $\ell = \mathrm{II}$, and then apply Lemma 4.

Finally note that the more complicated sums over the sequences of PRN's of type (I) and (II) may be investigated.

References

[1] **Eichenauer, J. and J. Lehn,** A non-linear congruential pseudorandom number generator, *Statist. Hefte*, **27** (1986), 315–326.

[2] **Niederreiter, H.,** Some new exponential sums with applications to pseudo-random numbers, In: *Topics in Number Theory* (*Debrecen, 1974*), Colloq. Math. Soc. János Bolyai, North-Holland, Amsterdam, **13** (1976), 209–232.

[3] **Niederreiter, H.,** On the cycle structure of linear recurring sequences, *Math. Scand*, **38** (1976), 53–77.

[4] **Niederreiter, H.,** On the distribution of pseudo-random numbers generated by the linear congruential method, III, *Math. Comp*, **30** (1976), 571–597.

[5] **Stoneham, R.G.,** On the uniform ε-distribution of residue within the periods of rational fractions with applications to normal numbers, *Acta Arith*, **22** (1973), 371–389.

[6] **Varbanets, Pavel and Sergey Varbanets,** Inversive generator of the second order with a variable shift for the sequence of PRNs, *Annales Univ. Sci. Budapest., Sect. Comp*, **46** (2017), 255-273.

[7] **Tran Kim Thanh, Tran The Vinh and Varbanets Sergey,** Generalization of inversive congruential generator with a variable shift, 11th CHAOS 2018 International Conference Proceedings, 5-8 June 2018, Rome, Italy, 2018 (to appear).

Sergey Varbanets
Department of Computer Algebra and Discrete Mathematics
I.I. Mechnikov Odessa National University
Odessa, 65026
Ukraine
varb@sana.od.ua