MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 198
APRIL 1992, PAGES 775-779

LOWER BOUNDS FOR THE DISCREPANCY OF INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS WITH POWER OF TWO MODULUS

JÜRGEN EICHENAUER-HERRMANN AND HARALD NIEDERREITER

ABSTRACT. The inversive congruential method with modulus $m = 2^{\omega}$ for the generation of uniform pseudorandom numbers has recently been introduced. The discrepancy $D_{m/2}^{(k)}$ of k-tuples of consecutive pseudorandom numbers generated by such a generator with maximal period length $m/2$ is the crucial quantity for the analysis of the statistical independence properties of these pseudorandom numbers by means of the serial test. It is proved that for a positive proportion of the inversive congruential generators with maximal period length, the discrepancy $D_{m/2}^{(k)}$ is at least of the order of magnitude $m^{-1/2}$ for all $k \geq 2$. This shows that the bound $D_{m/2}^{(2)} = O(m^{-1/2}(\log m)^2)$ established by the second author is essentially best possible.

1. INTRODUCTION AND NOTATION

In the last years inversive congruential pseudorandom number generators have been introduced and analyzed (cf. [1, 2, 3, 4]) as alternatives to linear congruential generators. The latter generators show too much regularity in the distribution of k-tuples of consecutive pseudorandom numbers for certain simulation purposes [1]. In the present paper the inversive congruential method with power of two modulus is considered.

Let $m = 2^{\omega}$ for some integer $\omega \geq 6$, $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$, and write G_m for the set of all odd integers in $\mathbb{Z}_m$. For $c \in G_m$, let $\overline{c} \in G_m$ be the multiplicative inverse of c modulo m, i.e., $\overline{c}$ is the unique element of G_m with $c\overline{c} \equiv 1 \pmod{m}$. Let $a, b, y_0 \in \mathbb{Z}_m$ be integers with $a \equiv 1 \pmod{4}$, $b \equiv 2 \pmod{4}$, and $y_0 \in G_m$. Define a sequence $(y_n)_{n\geq 0}$ of elements of G_m by the recursion

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{m}, \qquad n \geq 0. \tag{1}$$

A sequence $(x_n)_{n\geq 0}$ of uniform pseudorandom numbers is obtained by setting $x_n = y_n/m$ for $n \geq 0$. The numbers x_n, $n \geq 0$, are called *inversive congruential pseudorandom numbers*. It has been shown in [2] that the sequence $(y_n)_{n\geq 0}$ is purely periodic with period length $m/2$, and that $\{y_0, y_1, \dots, y_{(m/2)-1}\} = G_m$.

Received May 3, 1990.
1991 *Mathematics Subject Classification*. Primary 65C10; Secondary 11K45.
Key words and phrases. Pseudorandom number generator, inversive congruential method, power of two modulus, discrepancy.

The behavior of these pseudorandom numbers under the *k-dimensional serial test* for the full period has been investigated in [3] for $k = 2$. This test employs the discrepancy of k-tuples of consecutive pseudorandom numbers. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^k$, the *discrepancy* is defined by

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^k$, $F_N(J)$ is N^{-1} times the number of terms among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and $V(J)$ denotes the k-dimensional volume of J. If $(x_n)_{n\geq 0}$ is a sequence of inversive congruential pseudorandom numbers with modulus m and period length $m/2$, then the points

$$\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+k-1}) \in [0, 1)^k, \qquad 0 \leq n < m/2,$$

are considered and

$$D_{m/2}^{(k)} = D_{m/2}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{(m/2)-1})$$

is written for their discrepancy. It has been proved in [3] that

$$D_{m/2}^{(2)} = O(m^{-1/2}(\log m)^2),$$

where the implied constant is absolute.

In the present paper it is shown that for a given modulus m there exist multipliers a in the inversive congruential method (1) such that the discrepancy $D_{m/2}^{(k)}$ is at least of the order of magnitude $m^{-1/2}$ for all dimensions $k \geq 2$ and all increments b. Therefore, the upper bound $D_{m/2}^{(2)} = O(m^{-1/2}(\log m)^2)$ is in general best possible up to the logarithmic factor. Similar results for inversive congruential generators with prime modulus have been obtained recently in [4].

2. Auxiliary results

In the following the abbreviation $e(u) = e^{2\pi i u}$ for $u \in \mathbb{R}$ is used, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$. A proof of Lemma 1 is given in [4].

Lemma 1. *Let* $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ *be* N *arbitrary points in* $[0, 1)^k$ *with discrepancy* $D_N = D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1})$. *Then*

$$\left|\sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n)\right| \leq \frac{2}{\pi}\left(\left(\frac{\pi+1}{2}\right)^l - \frac{1}{2^l}\right) N D_N \prod_{j=1}^{k} \max(1, 2|h_j|)$$

for any nonzero vector $\mathbf{h} = (h_1, \ldots, h_k) \in \mathbb{Z}^k$, *where* l *is the number of nonzero coordinates of* $\mathbf{h}$.

Let $H_m = \{a \in \mathbb{Z}_m | a \equiv 1 \pmod 8\}$ be a subset of the set of admissible multipliers in the inversive congruential method (1). For integers c, put $\chi(c) = e(c/m)$ and

$$L_\chi(c) = \sum_{a \in H_m} \chi(ac).$$

A straightforward calculation shows that

$$L_\chi(c) = \begin{cases} \frac{m}{8}\chi(c) & \text{for } 8c \equiv 0 \pmod{m}, \\ 0 & \text{for } 8c \not\equiv 0 \pmod{m}. \end{cases} \tag{2}$$

Lemma 2. *If* c, $d \in G_m$ *with* $8(c+d) \equiv 0 \pmod{m}$, *then* $\chi(c+d)\chi(\overline{c}+\overline{d}) = 1$.

Proof. Let c, $d \in G_m$ with $8(c+d) \equiv 0 \pmod{m}$. Then there exists an integer $j \in \{0, 1, \dots, 7\}$ with $d \equiv j(m/8) - c \pmod{m}$. Since $c \equiv \overline{c} \pmod{8}$ and $m \geq 64$, it follows that $\overline{d} \equiv -j(m/8) - \overline{c} \pmod{m}$. Hence, $\overline{c} + \overline{d} \equiv -(c+d) \pmod{m}$, which yields $\chi(c+d)\chi(\overline{c}+\overline{d}) = 1$. □

Observe that for integers c, $d \in G_m$ the condition $8(c+d) \equiv 0 \pmod{m}$ is equivalent to $8(\overline{c}+\overline{d}) \equiv 0 \pmod{m}$. For integers a, define

$$K_\chi(a) = \sum_{c \in G_m} \chi(c + a\overline{c}).$$

Note that $K_\chi(a)$ is always real, which can be seen by changing c into $-c$ in the summation.

Lemma 3. *There holds*

$$\sum_{a \in H_m} (K_\chi(a))^2 = \frac{m^2}{2}.$$

Proof. An application of equation (2) and Lemma 2 yields

$$\begin{aligned} \sum_{a \in H_m} (K_\chi(a))^2 &= \sum_{a \in H_m} \sum_{c, d \in G_m} \chi(c + d + a(\overline{c} + \overline{d})) \\ &= \sum_{c, d \in G_m} \chi(c+d) L_\chi(\overline{c} + \overline{d}) \\ &= \frac{m}{8} \sum_{\substack{c, d \in G_m \\ 8(\overline{c}+\overline{d}) \equiv 0 \pmod{m}}} \chi(c+d)\chi(\overline{c}+\overline{d}) = \frac{m^2}{2}. \quad \square \end{aligned}$$

Lemma 4. *Let* $0 < t \leq 2$. *Then there are more than* $A(t)m/8$ *values of* $a \in H_m$ *for which* $|K_\chi(a)| \geq tm^{1/2}$, *where* $A(t) = (4 - t^2)/(8 - t^2)$.

Proof. The lemma will be proved by contradiction. Suppose that $|K_\chi(a)| \geq tm^{1/2}$ for at most $A(t)m/8$ values of $a \in H_m$. Then $|K_\chi(a)| < tm^{1/2}$ for at least $(1 - A(t))m/8$ values of $a \in H_m$. Now observe that $K_\chi(a)$ coincides with the Kloosterman sum $S(1, a; m)$ as defined by Salié [5]. Hence, it follows from results of Salié [5] that $|K_\chi(a)| \leq \sqrt{8}m^{1/2}$ for all $a \in H_m$. Therefore,

$$\sum_{a \in H_m} (K_\chi(a))^2 < (1 - A(t))\frac{t^2 m^2}{8} + A(t)m^2 = \frac{m^2}{2},$$

which is a contradiction to Lemma 3. □

3. Lower bounds for the discrepancy $D_{m/2}^{(k)}$

The main results of the present paper are summarized in the following two theorems.

Theorem 1. *Let* $m = 2^\omega$ *with* $\omega \geq 6$, *and let* $0 < t \leq 2$. *Then there exist more than* $A(t)m/8$ *multipliers* $a \in \mathbb{Z}_m$ *with* $a \equiv 1 \pmod 8$ *such that for all increments* $b \in \mathbb{Z}_m$ *with* $b \equiv 2 \pmod 4$ *the discrepancy of the corresponding inversive congruential generator* (1) *satisfies*

$$D_{m/2}^{(k)} \geq \frac{t}{\pi + 2} m^{-1/2}$$

for all dimensions $k \geq 2$, *where* $A(t) = (4 - t^2)/(8 - t^2)$.

Proof. First, Lemma 1 is applied with $k \geq 2$, $N = m/2$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < m/2$, and $\mathbf{h} = (1, 1, 0, \dots, 0) \in \mathbb{Z}^k$. This yields

$$\begin{aligned}(\pi + 2) m D_{m/2}^{(k)} &\geq \left| \sum_{n=0}^{m/2-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = \left| \sum_{n=0}^{m/2-1} e\left(\frac{1}{m}(y_n + y_{n+1})\right) \right| \\ &= \left| \sum_{n=0}^{m/2-1} \chi(y_n + a\overline{y}_n) \right| = |K_\chi(a)|.\end{aligned}$$

Now, the assertion follows from Lemma 4. □

Observe that according to Theorem 1 there exist inversive congruential generators (1) with maximal period length $m/2$ and

$$D_{m/2}^{(k)} \geq \frac{2}{\pi + 2} m^{-1/2}$$

for all dimensions $k \geq 2$.

Theorem 2. *Let* $m = 2^\omega$ *with* $\omega \geq 6$, *and let* $0 < t \leq 2$. *Then there exist more than* $A(t)m/8$ *multipliers* $a \in \mathbb{Z}_m$ *with* $a \equiv 5 \pmod 8$ *such that for all increments* $b \in \mathbb{Z}_m$ *with* $b \equiv 2 \pmod 4$ *the discrepancy of the corresponding inversive congruential generator* (1) *satisfies*

$$D_{m/2}^{(k)} \geq \frac{t}{3(\pi + 2)} m^{-1/2}$$

for all dimensions $k \geq 2$, *where* $A(t) = (4 - t^2)/(8 - t^2)$.

Proof. First, Lemma 1 is applied with $k \geq 2$, $N = m/2$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < m/2$, and $\mathbf{h} = (1, -3, 0, \dots, 0) \in \mathbb{Z}^k$. This yields

$$\begin{aligned}3(\pi + 2) m D_{m/2}^{(k)} &\geq \left| \sum_{n=0}^{m/2-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| = \left| \sum_{n=0}^{m/2-1} e\left(\frac{1}{m}(y_n - 3y_{n+1})\right) \right| \\ &= \left| \sum_{n=0}^{m/2-1} \chi(y_n - 3a\overline{y}_n) \right| = |K_\chi(-3a)|.\end{aligned}$$

Now, the assertion follows from Lemma 4, since $a \equiv 5 \pmod 8$ if and only if $-3a \equiv 1 \pmod 8$. □

BIBLIOGRAPHY

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

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

3. H. Niederreiter, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144.

4. ——, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287.

5. H. Salié, *Über die Kloostermanschen Summen* $S(u, v; q)$, Math. Z. **34** (1932), 91–109.

FACHBEREICH MATHEMATIK, TECHNISCHE HOCHSCHULE, SCHLOSSGARTENSTRASSE 7, D-6100 DARMSTADT, GERMANY

INSTITUTE FOR INFORMATION PROCESSING, AUSTRIAN ACADEMY OF SCIENCES, SONNENFELSGASSE 19, A-1010 VIENNA, AUSTRIA
E-mail address: nied@qiinfo.oeaw.ac.at