MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 206
APRIL 1994, PAGES 783–786

IMPROVED LOWER BOUNDS FOR THE DISCREPANCY OF INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS

JÜRGEN EICHENAUER-HERRMANN

ABSTRACT. The inversive congruential method with prime modulus for generating uniform pseudorandom numbers is studied. Lower bounds for the discrepancy of k-tuples of successive pseudorandom numbers are established, which improve earlier results of Niederreiter. Moreover, the present proof is substantially simpler than the earlier one.

1. INTRODUCTION AND MAIN RESULTS

A particularly promising approach of generating uniform pseudorandom numbers in the interval $[0, 1)$ is the inversive congruential method with prime modulus. A review of several nonlinear congruential methods is given in the survey articles [1, 5, 6] and in H. Niederreiter's excellent monograph [7].

Let $p \geq 5$ be a prime, and identify $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ with the finite field of order p. For $z \in \mathbf{Z}_p^* := \mathbf{Z}_p \backslash \{0\}$ let $\overline{z}$ denote the multiplicative inverse of z modulo p, and put $\overline{0} := 0$. For integers $a, c \in \mathbf{Z}_p^*$ an *inversive congruential sequence* $(y_n)_{n\geq 0}$ of elements of $\mathbf{Z}_p$ is defined by

$$y_{n+1} \equiv ac^2\overline{y}_n + c \pmod{p}, \qquad n \geq 0.$$

A sequence $(x_n)_{n\geq 0}$ of *inversive congruential pseudorandom numbers* in the interval $[0, 1)$ is obtained by $x_n = y_n/p$ for $n \geq 0$. Observe that these sequences are always purely periodic. In [2], sequences having maximal period length p are characterized. In particular, it follows from [2, Theorem 2] that this property depends only on $a \in \mathbf{Z}_p^*$, but not on the specific value of $c \in \mathbf{Z}_p^*$. Let $\mathbf{M}_p^*$ be the set of all $a \in \mathbf{Z}_p^*$ which belong to inversive congruential sequences with maximal period length p.

For assessing statistical independence properties the *discrepancy* of the k-tuples

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

of successive inversive congruential pseudorandom numbers can be used, which is defined by

$$D_p^{(k)} = \sup_J |F_p(J) - V(J)|,$$

Received by the editor December 14, 1992.
1991 *Mathematics Subject Classification*. Primary 65C10; Secondary 11K45.
Key words and phrases. Uniform pseudorandom numbers, inversive congruential method, prime modulus, discrepancy.

where the supremum is extended over all subintervals J of $[0, 1)^k$, $F_p(J)$ is p^{-1} times the number of points among $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1}$ falling into J, and $V(J)$ denotes the k-dimensional volume of J. The following two theorems from [4] provide lower bounds for $D_p^{(k)}$. Let φ be Euler's totient function and $\omega(m)$ be the number of different prime factors of a positive integer m. Let

$$t(p) = \left(1 - \frac{1}{p}(p^{1/2} + 2)2^{\omega(p-1)}\right)^{1/2}$$

and

$$A_p(t) = \frac{(1-t^2)p - (p^{1/2}+2)2^{\omega(p-1)}}{(4-t^2)p + 4p^{1/2} + 1}$$

for $0 < t \leq t(p)$. Note that [2, Corollary 1] implies that an inversive congruential sequence has maximal period length p if $z^2 - cz - ac^2$ is a primitive polynomial over $\mathbf{Z}_p$.

Theorem 1. *There are at least $\varphi(p+1)$ primitive polynomials $z^2 - cz - ac^2$ over $\mathbf{Z}_p$ such that the discrepancy $D_p^{(k)}$ for the corresponding inversive congruential generator satisfies*

$$D_p^{(k)} > \frac{1}{2(\pi+2)}(p^{-1/2} - 2p^{-3/5})$$

for all dimensions $k \geq 2$.

Theorem 2. *Let $0 < t \leq t(p)$. Then there are more than $A_p(t)\varphi(p^2-1)/2$ primitive polynomials $z^2 - cz - ac^2$ over $\mathbf{Z}_p$ such that the discrepancy $D_p^{(k)}$ for the corresponding inversive congruential generator satisfies*

$$D_p^{(k)} > \frac{t}{2(\pi+2)}p^{-1/2}$$

for all dimensions $k \geq 2$.

In the present paper the following improved lower bounds for $D_p^{(k)}$ are established. These results have two main advantages. They apply to all inversive congruential sequences with maximal period length p and not only to those belonging to a primitive polynomial, and they provide information on the subclasses of inversive congruential generators which correspond to the different values of $a \in \mathbf{M}_p^*$. Moreover, the proof of these results, which is given in the third section, is much simpler than the one of Theorems 1 and 2 in [4]. Let

$$\tilde{t}(p) = \left(\frac{p-3}{p-1}\right)^{1/2}$$

and

$$\widetilde{A}_p(t) = \frac{(1-t^2)p - 2p(p-1)^{-1}}{(4-t^2)p + 4p^{1/2} + 1}$$

for $0 < t \leq \tilde{t}(p)$.

Result 1. *Let $a \in \mathbf{M}_p^*$. Then there exists a $c \in \mathbf{Z}_p^*$ such that the discrepancy $D_p^{(k)}$ for the corresponding inversive congruential generator satisfies*

$$D_p^{(k)} \geq \frac{\tilde{t}(p)}{2(\pi+2)}p^{-1/2}$$

for all dimensions $k \geq 2$.

Result 2. *Let* $0 < t \leq \tilde{t}(p)$ *and* $a \in \mathbf{M}_p^*$. *Then there are more than* $\widetilde{A}_p(t)(p-1)$ *values of* $c \in \mathbf{Z}_p^*$ *such that the discrepancy* $D_p^{(k)}$ *for the corresponding inversive congruential generator satisfies*

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

for all dimensions $k \geq 2$.

2. Auxiliary results

First, some further notation is necessary. Let $e(t) = e^{2\pi i t}$ for $t \in \mathbb{R}$ and $\chi(z) = e(z/p)$ for $z \in \mathbf{Z}$. For fixed $a \in \mathbf{Z}_p^*$ and $c \in \mathbf{Z}_p$, an exponential sum is defined by

$$S(c) = \sum_{y \in \mathbf{Z}_p} \chi(c(y + a\overline{y})).$$

Lemma 1. *Let* $a \in \mathbf{Z}_p^*$. *Then*

$$\sum_{c \in \mathbf{Z}_p^*} |S(c)|^2 \geq p(p-3).$$

Proof. Easy calculations show that

$$\begin{aligned}
\sum_{c \in \mathbf{Z}_p} |S(c)|^2 &= \sum_{c \in \mathbf{Z}_p} \sum_{y,\, z \in \mathbf{Z}_p} \chi(c(y - z + a(\overline{y} - \overline{z}))) \\
&= \sum_{y,\, z \in \mathbf{Z}_p} \sum_{c \in \mathbf{Z}_p} \chi(c(y - z + a(\overline{y} - \overline{z}))) \\
&= p \cdot \#\{(y, z) \in \mathbf{Z}_p \times \mathbf{Z}_p | y - z + a(\overline{y} - \overline{z}) \equiv 0 \ (\operatorname{mod} p)\} \\
&\geq p(\#\{(y, z) \in \mathbf{Z}_p^* \times \mathbf{Z}_p^* | (y - z)(1 - a\overline{y}\,\overline{z}) \equiv 0 \ (\operatorname{mod} p)\} + 1) \\
&= p(\#\{(y, z) \in \mathbf{Z}_p^* \times \mathbf{Z}_p^* | y = z \text{ or } y \equiv a\overline{z} \ (\operatorname{mod} p)\} + 1) \\
&\geq p(2p - 3),
\end{aligned}$$

where the last inequality follows from the fact that there are at most two values of $z \in \mathbf{Z}_p^*$ with $z \equiv a\overline{z} \ (\operatorname{mod} p)$. Since $S(0) = p$, one obtains at once

$$\sum_{c \in \mathbf{Z}_p^*} |S(c)|^2 \geq p(2p-3) - p^2 = p(p-3). \quad \square$$

Lemma 2. *Let* $0 < t \leq \tilde{t}(p)$ *and* $a \in \mathbf{Z}_p^*$. *Then there are more than* $\widetilde{A}_p(t)(p-1)$ *values of* $c \in \mathbf{Z}_p^*$ *such that*

$$|S(c)| \geq t p^{1/2}.$$

Proof. The lemma is proved by contradiction. Suppose that $|S(c)| \geq tp^{1/2}$ for at most $\widetilde{A}_p(t)(p-1)$ values of $c \in \mathbf{Z}_p^*$. Then $|S(c)| < tp^{1/2}$ for at least $(1 - \widetilde{A}_p(t))(p-1)$ values of $c \in \mathbf{Z}_p^*$. Now, observe that $S(c) = K(\chi; c, ac) + 1$, where $K(\chi; \cdot, \cdot)$ denotes the Kloosterman sum defined in [3, Definition 5.42]. Hence, it follows from the classical bound for Kloosterman sums (cf. [3, Theorem 5.45]) that $|S(c)| \leq 2p^{1/2} + 1$ for all $c \in \mathbf{Z}_p^*$. Therefore, one obtains

$$\begin{aligned}\sum_{c \in \mathbf{Z}_p^*} |S(c)|^2 &< (1 - \widetilde{A}_p(t))(p-1)t^2 p + \widetilde{A}_p(t)(p-1)(2p^{1/2}+1)^2 \\ &= p(p-3),\end{aligned}$$

which is a contradiction to Lemma 1. □

3. Proof of the results

First, Lemma 1 in [4] is applied with $N = p$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < p$, $\mathbf{h} = (1, 1, 0, \dots, 0) \in \mathbf{Z}^k$, and hence $m = 2$. This yields

$$\begin{aligned} D_p^{(k)} &\geq \frac{1}{2(\pi+2)p} \left| \sum_{n=0}^{p-1} e(x_n + x_{n+1}) \right| \\ &= \frac{1}{2(\pi+2)p} \left| \sum_{n=0}^{p-1} \chi(y_n + ac^2 \overline{y}_n) \right| . \end{aligned}$$

Since $(y_n)_{n \geq 0}$ has maximal period length p, i.e., $\{y_0, y_1, \dots, y_{p-1}\} = \mathbf{Z}_p$, one obtains

$$D_p^{(k)} \geq \frac{1}{2(\pi+2)p} \left| \sum_{z \in \mathbf{Z}_p} \chi(z + ac^2 \overline{z}) \right| .$$

Now, the transformation $z \equiv cy \pmod p$ yields

$$D_p^{(k)} \geq \frac{1}{2(\pi+2)p} \left| \sum_{y \in \mathbf{Z}_p} \chi(c(y + a\overline{y})) \right| = \frac{1}{2(\pi+2)p} |S(c)| .$$

Therefore, Result 2 follows at once from Lemma 2. Finally, Result 1 is obtained from Result 2 with $t = \tilde{t}(p)$.

Bibliography

1. J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
2. M. Flahive and H. Niederreiter, *On inversive congruential generators for pseudorandom numbers*, Proc. Internat. Conf. on Finite Fields (Las Vegas, 1991), Dekker, New York, 1992, pp. 75–80.
3. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.
4. H. Niederreiter, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287.
5. ——, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345.
6. ——, *Nonlinear methods for pseudorandom number and vector generation*, Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems, vol. 374, Springer, Berlin, 1992, pp. 145–153.
7. ——, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992.

Fachbereich Mathematik, Technische Hochschule Darmstadt, Schlossgartenstrasse 7, D-64289 Darmstadt, Germany