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

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

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 \(a \in Z_p^*\), but not on the specific value of \(c \in Z_p^*\). Let \(M_p^*\) be the set of all \(a \in Z_p^*\) which belong to inversive congruential sequences with maximal period length \(p\).

For assessing statistical independence properties the discrepancy of the \(k\)-tuples

\[x_n = (x_n, x_{n+1}, \ldots, x_{n+k-1}) \in \{0, 1\}^k, \quad 0 \leq n < p,
\]
of successive inversive congruential pseudorandom numbers can be used, which is defined by

\[D_p^{(k)} = \sup_J |F_p(J) - V(J)|,\]
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 $x_0, x_1, \ldots, x_{p-1}$ 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 $\phi$ be Euler’s totient function and $\omega(m)$ be the number of different prime factors of a positive integer $m$. Let

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

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 $\mathbb{Z}_p$.

**Theorem 1.** There are at least $\phi(p+1)$ primitive polynomials $z^2 - cz - ac^2$ over $\mathbb{Z}_p$ 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 $A_p(t)\phi(p^2 - 1)/2$ primitive polynomials $z^2 - cz - ac^2$ over $\mathbb{Z}_p$ 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 $a \in M_p^*$. 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

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

and

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

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

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

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

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

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

for all dimensions $k \geq 2$.

**2. Auxiliary results**

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

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

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

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

**Proof.** Easy calculations show that

$$\sum_{c \in \mathbb{Z}_p^*} |S(c)|^2 = \sum_{c \in \mathbb{Z}_p^*} \sum_{y, z \in \mathbb{Z}_p} |\chi(c(y - z + a\bar{y} - \bar{z}))|$$

$$= \sum_{y, z \in \mathbb{Z}_p} \sum_{c \in \mathbb{Z}_p^*} |\chi(c(y - z + a\bar{y} - \bar{z}))|$$

$$= p \cdot \#\{(y, z) \in \mathbb{Z}_p^* \times \mathbb{Z}_p | y - z + a\bar{y} = 0 \pmod{p}\}$$

$$\geq p(\#\{(y, z) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* | y - z = 0 \pmod{p}\} + 1)$$

$$= p(\#\{(y, z) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* | y = z \text{ or } y = a\bar{z} \pmod{p}\} + 1)$$

$$\geq p(2p - 3),$$

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

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

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

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

**Proof.** The lemma is proved by contradiction. Suppose that $|S(c)| \geq tp^{1/2}$ for at most $\tilde{A}_p(t)(p - 1)$ values of $c \in \mathbb{Z}_p^*$. Then $|S(c)| < tp^{1/2}$ for at least $(1 - \tilde{A}_p(t))(p - 1)$ values of $c \in \mathbb{Z}_p^*$. 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 \(c \in \mathbb{Z}_p^*\). Therefore, one obtains

\[
\sum_{c \in \mathbb{Z}_p^*} |S(c)|^2 < (1 - \tilde{A}_p(t))(p - 1)t^2p + \tilde{A}_p(t)(p - 1)(2p^{1/2} + 1)^2
\]

\[= p(p - 3),\]

which is a contradiction to Lemma 1. \(\square\)

3. PROOF OF THE RESULTS

First, Lemma 1 in [4] is applied with \(N = p\), \(t_n = x_n\) for \(0 \leq n < p\), \(h = (1, 1, 0, \ldots, 0) \in \mathbb{Z}^k\), and hence \(m = 2\). This yields

\[
D_p^{(k)} \geq \frac{1}{2(\pi + 2)p} \left| \sum_{n=0}^{p-1} e(x_n + x_{n+1}) \right|
\]

\[= \frac{1}{2(\pi + 2)p} \left| \sum_{n=0}^{p-1} \chi(y_n + ac^2y_n) \right| .
\]

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

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

Now, the transformation \(z \equiv cy \pmod{p}\) yields

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

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

BIBLIOGRAPHY


FACHBEREICH MATHEMATIK, TECHNISCHE HOCHSCHULE DARMSTADT, SCHLOSSGARTENSTRASSE 7, D–64289 DARMSTADT, GERMANY