STATISTICAL INDEPENDENCE OF LINEAR CONGRUENTIAL PSEUDO-RANDOM NUMBERS

BY HARALD NIEDERREITER

Communicated by J. T. Schwartz, June 5, 1976

Given a modulus \( m \geq 2 \) and a multiplier \( \lambda \) relatively prime to \( m \), a sequence \( y_0, y_1, \ldots \) of integers in the least residue system mod \( m \) is generated by the recursion \( y_{n+1} \equiv \lambda y_n \pmod{m} \) for \( n = 0, 1, \ldots \), where the initial value \( y_0 \) is relatively prime to \( m \). The sequence \( x_0, x_1, \ldots \) in the interval \([0, 1)\), defined by \( x_n = y_n/m \) for \( n = 0, 1, \ldots \), is then a sequence of pseudo-random numbers generated by the linear congruential method. The sequence is periodic, with the least period \( \tau \) being the exponent to which \( \lambda \) belongs mod \( m \).

For fixed \( s \geq 2 \), consider the \( s \)-tuples \( x_{n,s} = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \), \( n = 0, 1, \ldots \). We determine the empirical distribution of the \( s \)-tuples \( x_0, x_1, \ldots \) and compare it with the uniform distribution on \([0, 1]^s\). The original sequence \( x_0, x_1, \ldots \) of linear congruential pseudo-random numbers passes the serial test (for the given value of \( s \)) if the deviation between these two distributions is small. To measure this deviation, we introduce the quantity

\[
D_N = \sup_J |F_N(J) - V(J)| \quad \text{for } N \geq 1,
\]

where the supremum is extended over all subintervals \( J \) of \([0, 1]^s\), \( F_N(J) \) is \( N^{-1} \) multiplied by the number of terms among \( x_0, x_1, \ldots, x_{N-1} \) falling into \( J \), and \( V(J) \) denotes the volume of \( J \).

For a nonzero lattice point \( h = (h_1, \ldots, h_s) \in \mathbb{Z}^s \), let \( r(h) \) be the absolute value of the product of all nonzero coordinates of \( h \). We set

\[
R(s)(\lambda, m, q) = \sum_{h \equiv 0(q)} \frac{1}{(r(h))^{-1}},
\]

where the sum is extended over all nonzero lattice points \( h \) with \(-m/2 < h_j \leq m/2 \) for \( 1 \leq j \leq s \) and \( h \cdot \lambda \equiv h_1 + h_2 \lambda + \cdots + h_s \lambda^{s-1} \equiv 0 \pmod{q} \). For prime moduli \( m \), a somewhat simplified version of our result reads as follows.

**Theorem 1.** For a prime \( m \) and for a multiplier \( \lambda \) belonging to the exponent \( \tau \pmod{m} \), we have

\[
AMS (MOS) \text{ subject classifications (1970). Primary 65C10, 68A55; Secondary 10G05, 10K05.}
\]

\[1 \] This research was supported by NSF Grant MPS72-05055 A02 at the Institute for Advanced Study, Princeton, New Jersey, in the academic year 1974-1975.

Copyright © 1976, American Mathematical Society
\[ D_\tau < \frac{s}{m} + \min \left( \left( 1, \frac{\sqrt{m - \tau}}{\tau} \right), \left( \frac{2}{\pi} \log m + \frac{7}{5} \right)^s + \frac{1}{2} R^{(s)}(\lambda, m, m) \right). \]

The second term in the upper bound is nonincreasing as a function of \( \tau \) and so becomes minimal for \( \tau = m - 1 \). Values of \( \lambda \) that minimize \( R^{(s)}(\lambda, m, m) \) are of fundamental importance in the theory of good lattice points in the sense of Korobov and Hlawka (see [2, Chapter 2, §5]). We conclude that a multiplier \( \lambda \) is favorable with regard to the \( s \)-dimensional serial test if \( \lambda = (1, \lambda, \ldots, \lambda^{s-1}) \) is a good lattice point mod \( m \) (or, equivalently, \( \lambda \) is an optimal coefficient mod \( m \)) and \( \lambda \) is a primitive root mod \( m \). It can be shown that there exist primitive roots \( \lambda_0 \) mod \( m \) for which \( R^{(s)}(\lambda_0, m, m) \) is of the order of magnitude \( m^{-1} \log^s m \log \log m \).

For an odd prime power \( m = p^\alpha \), \( p \) prime, \( \alpha \geq 2 \), and for \( |\lambda| > 1 \), let \( \tau(p) \) be the exponent to which \( \lambda \) belongs mod \( p \) and let \( \beta \) be the largest integer such that \( p^\beta \) divides \( \lambda^{\tau(p)} - 1 \).

**Theorem 2.** For an odd prime power modulus \( m = p^\alpha \) with \( \alpha \geq \beta \), we have

\[ D_\tau < \frac{s}{m} + \frac{1}{2} R^{(s)}(\lambda, m, p^{\alpha-\beta}). \]

**Theorem 3.** If \( m = 2^\alpha \) with \( \alpha \geq 3 \) and \( \lambda \equiv 5 \) (mod 8), then

\[ D_\tau < \frac{s}{m} + \frac{1}{2} R^{(s)}(\lambda, m, 2^{\alpha-2}). \]

If \( m = 2^\alpha \) with \( \alpha \geq 4 \) and \( \lambda \equiv 3 \) (mod 8), then

\[ D_\tau < \frac{s}{m} + \frac{1}{2} R^{(s)}(\lambda, m, 2^{\alpha-1}) + \frac{1}{2\sqrt{2}} \left( R^{(s)}(\lambda, m, 2^{\alpha-3}) - R^{(s)}(\lambda, m, 2^{\alpha-2}) \right). \]

Since the upper bounds in Theorems 2 and 3 can be estimated in terms of \( R^{(s)}(\lambda, m', m') \) with a suitable \( m' < m \), the remarks following Theorem 1 apply, *mutatis mutandis*, to prime power moduli.

For computational purposes, it is more convenient to replace \( R^{(s)}(\lambda, m, m) \) by the quantity

\[ \rho^{(s)}(\lambda, m) = \min_h r(h), \]

where the minimum is extended over the range of lattice points used in the definition of \( R^{(s)}(\lambda, m, m) \).

**Theorem 4.** For any dimension \( s \geq 2 \) and for any integers \( m \geq 2 \) and \( \lambda \), we have

\[ R^{(s)}(\lambda, m, m) < \rho^{-1}(\log 2)^{1-s}((2 \log m)^s + 4(2 \log m)^{s-1}) + \rho^{-1}2^{s+1}(2^{s-2} - 1) \left( \frac{k + s - 2}{s - 1} \right), \]

where \( \rho = \rho^{(s)}(\lambda, m) \) and \( k = \lfloor (\log m)/\log 2 \rfloor \).
There exists an interesting relationship between the two-dimensional serial test and continued fractions. It is based on the fact that \( R^{(2)}(\lambda, m, m) \) can be estimated in terms of the partial quotients in the expansion of \( \lambda/m \) into a finite simple continued fraction. As a consequence, one obtains that \( \lambda \) is favorable with regard to the distribution of pairs whenever these partial quotients are small. This is in accordance with results of Dieter [1] concerning the case \( s = 2 \).

The proofs of Theorems 1, 2 and 3 depend on estimates for exponential sums with linear recurring arguments established in [3]. The case of inhomogeneous linear congruential pseudo-random numbers and the serial test for parts of the period can be treated by similar techniques (see [5]).

Details and proofs, as well as further results, will appear in [4].

REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024

Current address: Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801