BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 82, Number 6, November 1976

STATISTICAL INDEPENDENCE OF LINEAR CONGRUENTIAL PSEUDO-RANDOM NUMBERS

BY HARALD NIEDERREITER[1]

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

Given a modulus $m \geqslant 2$ and a multiplier λ 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 τ being the exponent to which λ belongs mod m.

For fixed $s \geqslant 2$, consider the s-tuples $\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n = 0, 1, \ldots$. We determine the empirical distribution of the s-tuples $\mathbf{x}_0, \mathbf{x}_1, \ldots$ 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

$$D_N = \sup_J |F_N(J) - V(J)| \quad \text{for } N \geqslant 1,$$

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 $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ falling into J, and $V(J)$ denotes the volume of J.

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

$$R^{(s)}(\lambda, m, q) = \sum_{\substack{\mathbf{h} \ (\mathrm{mod}\ m) \\ \mathbf{h} \cdot \lambda \equiv 0(q)}} (r(\mathbf{h}))^{-1},$$

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

THEOREM 1. *For a prime m and for a multiplier λ belonging to the exponent τ* mod m, *we have*

AMS (MOS) subject classifications (1970). Primary 65C10, 68A55; Secondary 10G05, 10K05.

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