BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 2, March 1978

RESEARCH ANNOUNCEMENTS

THE SERIAL TEST FOR LINEAR CONGRUENTIAL PSEUDO-RANDOM NUMBERS

BY HARALD NIEDERREITER[1]

Communicated by Jack Schwartz, August 22, 1977

Let $m \geqslant 2$ and r be integers, let y_0 be an integer in the least residue system mod m, and let λ be an integer coprime to m with $\lambda \not\equiv \pm 1 \pmod{m}$ and $(\lambda - 1)y_0 + r \not\equiv 0 \pmod{m}$. A sequence $y_0, y_1, \ldots$ of integers in the least residue system mod m is generated by the recursion $y_{n+1} \equiv \lambda y_n + r \pmod{m}$ for $n = 0, 1, \ldots$. In the homogeneous case $r \equiv 0 \pmod{m}$, one chooses y_0 to be coprime 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 a sequence of linear congruential pseudo-random numbers. The sequence is purely periodic; let τ denote its least period. In practice, m is taken to be a large prime or a large power of 2.

For a given $s \geqslant 2$, the serial test is set up to determine the amount of statistical dependence among s successive terms in the sequence $x_0, x_1, \ldots$. To this end, one considers the s-tuples $\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n = 0, 1, \ldots$, and measures the deviation between the empirical distribution of the first N of these s-tuples and the uniform distribution on $[0, 1]^s$ by the quantity D_N introduced in [3], where $1 \leqslant N \leqslant \tau$. For the homogeneous case, effective estimates for D_τ were established in [3], [4]. By extending techniques from [2] and [4], we can now handle the general case. Estimates for D_N with $N < \tau$ are of great practical interest because in calculations involving linear congruential pseudo-random numbers one only uses an initial segment of the period and not the full period itself.

The number $R^{(s)}(\lambda, m, q)$ is defined as in [3]. C_s will denote an explicitly known constant depending only on s, whose exact value may be different in each occurrence.

THEOREM 1. *For a prime m we have*

$$D_N < \begin{cases} \dfrac{s}{m} + \dfrac{C_s}{\tau}(m-\tau)^{1/2}(\log m)^s + \dfrac{1}{2}R^{(s)}(\lambda, m, m) & \text{for } N = \tau, \\ \dfrac{s}{m} + \dfrac{C_s}{N}m^{1/2}(\log m)^{s+1} + \dfrac{1}{2}R^{(s)}(\lambda, m, m) & \text{for } 1 \leqslant N \leqslant \tau. \end{cases}$$

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

[1]Supported by NSF Grant MCS 77-01699.