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*

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

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

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

Now let m be a prime power, say $m = p^\alpha$ with p prime and $\alpha \geqslant 2$. For $h \geqslant 1$, let $\mu(p^h)$ be the exponent to which λ belongs mod p^h. Define a positive integer β as follows: if p is odd, let β be the largest integer such that p^β divides $\lambda^{\mu(p)} - 1$; if $p = 2$, let β be the largest integer such that 2^β divides $\lambda^{\mu(4)} - 1$. Furthermore, let κ be the largest integer such that p^κ divides $\lambda - 1$, let ω be the largest integer such that p^ω divides $(\lambda - 1)y_0 + r$, and set $\gamma = \beta + \omega - \kappa$.

THEOREM 2. *For a prime power $m = p^\alpha$, p prime, $\alpha \geqslant 2$, and a λ with $\gamma < \alpha$ we have*

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

We note that in the frequently used special case $m = 2^\alpha$, $\lambda \equiv 5 \pmod 8$, and r odd we have $\gamma = 0$. The interpretation of these results is similar to that in [3], [4].

The quantity $\rho^{(s)}(\lambda, m)$ introduced in [3] is convenient for computational purposes. Because of the above results and [3, Theorem 4], the reciprocal of $\rho^{(s)}(\lambda, m)$ may be taken as a measure for the amount of statistical dependence among s successive terms in a sequence $x_0, x_1, \ldots$ having a large period τ. The fact that this is really the correct indicator is shown by the following result.

THEOREM 3. *For any m, λ, and N with $1 \leqslant N \leqslant \tau$* we have

$$D_N \geqslant \begin{cases} 1/s^s\rho^{(s)}(\lambda, m) & \textit{for } 2 \leqslant s \leqslant 6, \\ \pi/2(2\pi + 1)^s\rho^{(s)}(\lambda, m) & \textit{for } s \geqslant 7. \end{cases}$$

We remark that the estimates for D_N given here yield effective error bounds for Monte Carlo integrations using the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}$ as nodes. This follows from general inequalities for the integration error in terms of D_N which can be found in [1, Chapter 2, §5].

REFERENCES

1. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley, New York, 1974.

2. H. Niederreiter, *On the distribution of pseudo-random numbers generated by the linear congruential method*. III, Math. Comp. 30 (1976), 571–597.

3. ———, *Statistical independence of linear congruential pseudo-random numbers*, Bull. Amer. Math. Soc. 82 (1976), 927–929.

4. ———, *Pseudo-random numbers and optimal coefficients*, Advances in Math. 26 (1977), 99–181.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, ILLINOIS 61801