Proceedings of the 1984
Winter Simulation Conference
S. Sheppard, U. Pooch, D. Pegden (eds.)

AN EXHAUSTIVE SEARCH FOR OPTIMAL MULTIPLIERS

George S. Fishman, Professor & Chairman of the Curriculum in Operations Research and Systems Analysis, University of North Carolina, Chapel Hill, North Carolina 27514

Louis R. Moore, Assistant Professor, Operations Research and Systems Analysis, University of North Carolina, Chapel Hill, North Carolina 27514

This paper presents the results of an exhaustive search to find optimal multipliers A for the multiplicative congruential random number generator $Z_i \equiv A\ Z_{i-1} \pmod{M}$ with prime modulus $M = 2^{31} - 1$. Since Marsaglia (1968) has shown that k-tuples from this and the more general class of linear congruential generators lie on sets of parallel hyperplanes, it has become common practice to evaluate multipliers in terms of their induced hyperplane structures. This study continues the practice and regards a multiplier as optimal if for $k = 2,\ldots,6$ and each set of parallel hyperplanes the Euclidean distance between adjacent hyperplanes does not exceed the minimal achievable distance by more than a prespecified amount. The concept of using this distance measure to evaluate multipliers orginated in the spectral test of Coveyou and MacPherson (1967) and has been used notably by Knuth (1981). However, the criterion of optimality defined here is considerably more stringent than the criteria that these writers proposed.

First proposed by Lehmer (1951), the multiplicative congruential random number generator has come to be the most commonly employed mechanism for generating random numbers. Jannson (1966) collected the then known properties of these generators. Shortly thereafter Marsaglia (1968) showed that all such generators share a common theoretical flaw and Coveyou and MacPherson (1967), Beyer, Roof and Williamson (1971), Marsaglia (1972) and Smith (1971) proposed alternative procedures for rating the seriousness of this flaw for individual multipliers. Later Niederreiter (1976, 1977, 1978a,b) proposed a rating system based on the concept of discrepancy, a measure of error used in numerical integration. With regard to empirical evaluation, Fishman and Moore (1982) described a comprehensive battery of statistical tests and illustrated how they could be used to detect local departures from randomness in samples of moderate size taken from these generators.

Although the theoretical rating procedures have existed for some time, with the exception of Hoaglin (1976), Ahrens and Dieter (1977) and Knuth (1981), little use has been made of them. The present study, by its sheer exhaustiveness, removes this deficiency for generators with $M = 2^{31} - 1$. The worst case performance measures that have been proposed to rate generators in k dimensions include the maximal distance between adjacent parallel hyperplanes, the minimal number of parallel hyperplanes, the minimal distance between k-tuples, and the discrepancy. The best multipliers for the modulus and their performances for all these measures are presented. Lattice packing measures are presented and the given multipliers perform well with respect to these measures. Also, the packing measures in the dual space are identical with Knuth's figure of merit for evaluating generators. Our results indicate that with regard to this criterion, the five best multipliers for $M = 2^{31} - 1$ perform better than all 30 multipliers listed in Table 1 of Knuth (1981, pp. 102-103). Bounds on discrepancy are also computed and discussed. The results of a comprehensive empirical analysis of the local sampling properties of the best multipliers, using the procedures in Fishman and Moore (1982), indicate no evidence of departures from randomness.

REFERENCES

Ahrens, J. H. and U. Dieter (1977). Uniform Random Numbers, University of Graz.

Anderson, T. W. and D. A. Darling (1952). "Asymptotic Theory of Goodness of Fit Criteria Based on Stochastic Processes," Ann. Math. Statist., 23, 1983-212.

Anderson, T. W. and D. A. Darling (1954). "A Test of Goodness of Fit," J. Amer. Statist. Assoc., 49, 765-769.

Beyer, W. A., R. B. Roof and D. Williamson (1971). "The Lattice Structure of Multiplicative Congruential Pseudo-Random Vectors," Mathematics of Computation, 25, 345-363.

Borosh, S. and H. Niederreiter (1983). "Optimal Multipliers for Pseudo-random Number Generation by The Linear Congruential Method." Bit, 23, 65-74.

Cassels, J. W. S. (1959). An Introduction to the Geometry of Numbers, Springer-Verlag.

Coveyou, R. R. (1970). "Random Number Generation is Too Important to be Left to Chance," Studies in Appl. Math., 3, 70-111.

Coveyou, R. R. and R. D. MacPherson (1967). "Fourier Analysis of Uniform Random Number Generators," J. Assoc. Comput. Mach., 14, 100-119.

Dwass, M. (1958). "On Several Statistics Related to Empirical Distribution Functions," Ann. Math. Statist. 29, 188-191.

Dieter, U. (1971). "Pseudo-random Numbers: The Exact Distribution of Pairs," Math. Comp., 25, 855-883.

Dieter, U. (1975). "How to Calculate Shortest Vectors in a Lattice," Mathematics of Computation, 29, 827-833.

Fishman, G. S. and L. R. Moore (1982). "A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus $2^{31} - 1$." J. Amer. Statist. Assoc., 77, 129-136.

Hardy, G. H. and E. M. Wright (1960). The Theory of Numbers, 4th ed. Oxford: Clarendon Press.

Hoaglin, D. (1976). "Theoretical Properties of Congruential Random-Number Generators: An Empirical View," Memorandum NS-340, Department of Statistics, Harvard University.

IMSL (1980). IMSL Library Reference Manual, Edition 8, IMSL INC., Houston, Texas.

Jannson, B. (1966). Random Number Generators, Stockholm: Almqvist and Wiksell.

Katzan, H., Jr. (1971). APL Users Guide, Van Nostrand Reinhold, New York.

Kiviat, P., R. Villanueva and H. Markowitz (1969). The SIMSCRIPT II Programming Language, Prentice-Hall.

Knuth, D. E. (1981). The Art of Computer Programming: Semi-numerical Algorithms, second ed., Addison-Wesley.

Lehmer, D. H. (1981). "Mathematical Methods in Large Scale Computing Units," Ann. Comp. Labs., Harvard University, 26, 141-146.

Marsaglia, G. (1968). "Random Numbers Fall Mainly in the Plane," Proc. Nat. Acad. Sci., 61, 25-28.

Marsaglia, G. (1972). "The Structure of Linear Congruential Sequences," in Applications of Number Theory to Numerical Analysis, ed. S. K. Zarenba, New York: Academic Press.

Neiderreiter, H. (1976). "Statistical Independence of Linear Congruential Pseudo-random Numbers," Bull. Amer. Math. Soc., 82, 927-929.

Neiderreiter, H. (1977). "Pseudo-random Numbers and Optimal Coefficients." Advances in Math. 26, 99-181.

Neiderreiter, H. (1978a). "The Serial Test for Linear Congruential Pseudo-random Numbers," Bull Amer. Math. Soc., 84, 273-274.

Neiderreiter, H. (1978b). "Quasi-Monte Carlo Methods and Pseudo-random Numbers," Bull. Amer. Math. Soc., 84, 957-1040.

Payne, W. H., J. R. Rabung and T. P. Bogyo (1969). "Coding the Lehmer Pseudo-random Number Generator," Comm. A&M, 12, 85-86.

SAS Institute Inc. (1982). SAS User's Guide: Basics, Cary, North Carolina.

Smith, C. S. (1971). "Multiplicative Pseudo-Random Number Generators with Prime Modulus," J. ACM, 18, 586-593.