

Criterion of Spectral Test for Linear Congruential Random Number Generators

Ching-Jing Kung¹ and Hui-Chin Tang^{2*}

¹*Department of Industrial Engineering and Management, Cheng Shiu University,
Kaohsiung, Taiwan 833, R.O.C.*

²*Department of Industrial Engineering and Management, National Kaohsiung University of Applied Sciences,
Kaohsiung, Taiwan 807, R.O.C.*

Abstract

The criterion issue of spectral test in a linear congruential random number generator is considered. In this paper, we report on four variants of the normalized spectral test, measured both relative to either a theoretical or exact lower bound and aggregative to either a worst-case or average-case method. Computer exhaustive searches are conducted to evaluate and compare their statistical behaviors. It is shown that the spectral test with both theoretical lower bound and average-case aggregation criterion outperforms.

Key Words: Linear Congruential Generator, Spectral Test, Random Number

1. Introduction

The problem of generating a sequence of independent and uniform random numbers (RNs) often arises in varied applications. Since the publication of Lehmer's paper in 1951 [1], various approaches have been proposed for the RN generation problem. These approaches can be classified into four categories: k th-order multiple recursive generator (MRG), generalized feedback shift register generator, inverse generator, and combined generator. Three extensive surveys of the theory, implementation and applications of various approaches are given by Fishman [2], Knuth [3], and Niederreiter [4]. A k th-order MRG has been a useful and popular methodology for generating near-ideal RNs in a wide variety of RN generation approaches. An interesting special case is when the order is one. Such MRG is the well-known linear congruential generator (LCG) [5] of the form

$$R_n \equiv a_1 R_{n-1} \pmod{m} \quad (1)$$

where m is the prime modulus, a is the constant multi-

plier, and R_0 is the constant seed. The theory of LCG is one of the oldest parts of RN generation as well as one particularly rich in applications, so it has been by far the most extensively studied and developed.

Full period, randomness and efficient implementation are three prerequisite criteria for an ideal RN generator. The number of the maximum period of a RN generator is large enough so that such generators are easy to find. For a full period RN generator, the computer simulation practitioners and researchers place large emphasis on obtaining a sequence of independent and uniform RNs in the t -dimensional hypercube $(0,1)^t$, where t is a positive integer. Let T_t be the set of all possible overlapping t -tuples of successive RNs plus the zero-vector. The periodic continuation of T_t with period m forms a lattice L_t . Two evaluations of a lattice L_t have evolved in the literature: theoretical and empirical evaluations. For the empirical evaluation, a large amount of statistical tests have been suggested in the literature. These tests can be categorized to be of two basic types: (1) those that examine its independent behavior, (2) those that examine its uniform behavior. However, the main disadvantage of these statistical tests is that the computational cost required to find good RN generators via an exhaustive

*Corresponding author. E-mail: tang@cc.kuas.edu.tw

search would take years for computation. We now consider an alternative method, known as the theoretical evaluation. Several theoretical evaluations to assess the global randomness in a lattice L_t . They include: (1) maximal distance between adjacent parallel hyperplanes (spectral test); (2) ratio of lengths of longest and shortest minimal basis vectors (lattice test); (3) the maximal difference between the volumes of regions in the t -dimensional unit hypercube and in numerical integration (discrepancy); (4) minimal number of parallel hyperplanes; (5) minimal distance between points. Of which the spectral test [5] and lattice test [6] are two statistical powerful and computational efficient tests for evaluating randomness. To rate various dimensions and generators for the spectral test, Fishman and Moore [5] normalized between zero and one by a theoretical lower bound, and adopted the worst-case performance measure. Tang [7] conducted a comprehensive empirical comparison of the worst-case normalized spectral test and lattice test for the full period LCGs with unrestricted multipliers and full period second-order MRGs with restricted multipliers for modulus $m = 2^{31} - 1$. It reveals that the spectral test is the most efficient way of finding good MRGs. Tang [8] performed an exhaustive search for the best worst-case normalized spectral test in a full period LCG with both the largest prime modulus smaller than 2^b , for bit sizes $b = 8, 9, \dots, 31$ and the three types of restrictions on multipliers. All of literature [5–8] adopted the theoretical lower bound and worst-case performance measure for the spectral test. Although consideration of the theoretical lower bound and worst-case performance measure is intuitively appealing, another choice is the exact lower bound and average-case performance measure, respectively. It follows that there are four variants of the normalized spectral test. For each variant, this paper conducts an exhaustive search for good MRGs, and analyzes their results by a comprehensive range of statistical tests. Since the possible number of MRGs with order larger than one is extremely huge, an exhaustive analysis would take years for computation. As an illustration, the LCG with modulus $2^{31} - 1$ is studied in this paper.

This paper is organized as follows. We first describe the four variants of the normalized spectral test of a full period LCG. We then give detailed statistical tests and comparisons. Finally, some concluding remarks are made.

2. Criterion of Spectral Test

Before discussing the four variants of the normalized spectral test, we first provide a concise review of the full period and spectral test of an LCG. The maximum period of an LCG with prime modulus m is $(m - 1)$. An LCG with maximum period is called a full period LCG. A necessary and sufficient condition of obtaining a full period is that multiplier a is a primitive root modulo m . For 32-bit computers, the largest prime modulus representable as an ordinary integer is $m = 2^{31} - 1$. For such modulus, four properties of the primitive root are described here: (1) 5.346E8 multipliers are primitive roots, (2) the minimal primitive root is 7, (3) $7^b \pmod{m}$ is a primitive root for every integer b relatively prime to $m - 1 = 2 \times 3^2 \times 7 \times 11 \times 31 \times 151 \times 331$, and (4) $7^b \pmod{m}$ is a primitive root if and only if $7^{m-1-b} \pmod{m}$ is a primitive root.

The spectral test method, proposed by Coveyou and MacPherson [9], is one of the most useful and powerful tools in practice. We adopt the state-of-the-art algorithm proposed by Fincke and Pohst [10] to calculate the maximum distance d_t between adjacent parallel hyperplanes in L_t .

Two lower bounds on d_t are considered: theoretical and exact lower bounds. From the geometry of number, a theoretical lower bound on d_t is known exactly for $t \leq 8$ [11]

$$d_t^*(T) = \begin{cases} m^{-1/t} / \gamma_t & \text{if } t > 1 \\ 1/m & \text{if } t = 1 \end{cases} \quad (2)$$

where γ_t takes the respective values $(4/3)^{1/4}$, $2^{1/6}$, $2^{1/4}$, $2^{3/10}$, $(64/3)^{1/12}$, $2^{3/7}$, and $2^{1/2}$ for $t = 2, 3, 4, 5, 6, 7$, and 8. Secondly, since the discrete nature of the lattice structure, these lower bound values $d_t^*(T)$ cannot be attained by an LCG. The exact lower bounds $d_t^*(E)$ on d_t found from an exhaustive search [11] are $1/\sqrt{2478955520}$, $1/\sqrt{2091014}$, $1/\sqrt{64281}$, $1/\sqrt{7365}$, $1/\sqrt{1798}$, $1/\sqrt{675}$, and $1/\sqrt{355}$ for $t = 2, 3, 4, 5, 6, 7$, and 8, respectively.

In addition to defining the lower bound on d_t , the second issue is to specify the performance measure for the different dimension t . We can adopt those dimensions

which have the smallest spectral values to aggregate different dimensions. Thus, a worst-case performance measure $\min_{2 \leq t \leq 8} d_t^*(T) / d_t$ is adopted for the theoretical lower bound, and $\min_{2 \leq t \leq 8} d_t^*(E) / d_t$ for the exact lower bound. It would also be possible to use an average-case performance measure. An average-case performance measure is $\frac{1}{7} \sum_{t=2}^8 d_t^*(T) / d_t$ for the theoretical lower bound, and $\frac{1}{7} \sum_{t=2}^8 d_t^*(E) / d_t$ for the exact lower bound. These four performance measures are always between zero and one. The larger the performance measure is, the smaller empty slice in L_t is and vice versa. Consequently, we seek generators with these four performance measures close to one.

3. Computational Experience

We evaluate and compare four variants of the normalized spectral test for a full period LCG. The criterion of spectral test is denoted by $S(L, M)$, where L dictates the lower bound on d_t and M dictates the aggregation measure for different dimension t . We restrict our attention to $L \in \{T, E\}$, where T is the theoretical lower bound and E is the exact lower bound. Also, $M \in \{W, A\}$, where W is a worst-case performance measure and A is an average-case performance measure. Specifically, $S(T, W) = \min_{2 \leq t \leq 8} d_t^*(T) / d_t$, $S(T, A) = \frac{1}{7} \sum_{t=2}^8 d_t^*(T) / d_t$, $S(E, W) = \min_{2 \leq t \leq 8} d_t^*(E) / d_t$, and $S(E, A) = \frac{1}{7} \sum_{t=2}^8 d_t^*(E) / d_t$.

Since the computational times of the four variants of the spectral test with maximum $S(L, M)$ criterion are almost same, we adopt a statistical analysis to evaluate and compare their effectiveness. The number of LCGs that pass all the statistical tests can serve as a judging criterion for effectiveness. For the statistical tests, runs and auto-correlation of lags one, two and three statistics are chosen for testing statistical independence, while the chi-square and serial of dimensions two and three statistics for testing uniformity. In order to increase the power of statistical tests, we adopt a two-level procedure of L'Ecuyer [12]. More precisely, each statistical test is applied one thousand times on consecutive subsequences

of 2^{21} RNs, then the empirical distribution of these one thousand statistics is compared to the theoretical distribution via the Kolmogorov-Smirnov test. Therefore, seven two-level statistical tests are applied to compare the effectiveness of these four variants of the spectral test with maximum $S(L, M)$ criterion. In order to compare fairly, each two-level statistical test is conducted by using the same seed that has been randomly chosen.

To study the influence of criterion $S(L, M)$ on spectral test, an LCG with modulus $m = 2^{31} - 1$ is conducted. The independent variables are the lower bound (theory or exactness) and the method of aggregation (worst-case or average-case). The sole dependent variable is the best twenty LCGs found by an exhaustive search for full period LCGs with maximum $S(L, M)$ criterion. For each spectral test with maximum $S(L, M)$ criterion, the twenty good multipliers are shown in Table 1. Since there exists a pair of multipliers $(a, a^{-1} \bmod m)$ with the same spectral test, we only present the one multiplier in the Table 1. To our surprise, the twenty good LCGs found by $S(T, A)$ and $S(E, A)$ are all same, while those of $S(T, W)$ and $S(E, W)$ are all different. At the 0.05 significant level, the numbers of LCGs that pass the two-level statistical tests are summarized in Table 2, where AR_i denotes the auto-correlation test of lag i , CS the chi-square test, and $Serial\ i$ the serial test of dimension i . Detailed p -values are available from authors. The first salient feature is that the two methods which use an average-case performance measure yield better than their counterpart in which a worst-case performance is adopted. The second salient feature is that both $S(T, A)$ and $S(E, A)$ provide equally good performance, whereas for the worst-case performance measure, $S(T, W)$ and $S(E, W)$, the latter which uses the exact lower bound to be superior. Hence the evidence listed in Table 2 suggests that the spectral test with maximum $S(T, A)$ or $S(E, A)$ outperforms. However, the exact lower bound requires extra computational time to obtain. Therefore, the practical consideration may indicate that the spectral test with maximum $S(T, A)$ criterion is a good way of obtaining an ideal LCG.

4. Conclusion

This paper empirically analyzes the criterion of spectral test for a full period LCG. According to the lower bound of d_t and the aggregation measure of dimension t ,

Table 1. Exhaustive searches for the twenty good LCGs with respect to the spectral test with maximum $S(L, M)$ criterion

Multiplier	$S(T, W)$	Multiplier	$S(T, A)$	Multiplier	$S(E, W)$	Multiplier	$S(E, A)$
885300443	0.76657	1332582004	0.82535	756894484	0.83548	1332582004	0.87580
554271143	0.76297	293398871	0.82303	1101592370	0.83108	293398871	0.87496
588399478	0.76219	1691546765	0.82270	629824009	0.82837	1691546765	0.87371
379983904	0.76202	1754050460	0.82041	1801742154	0.82508	1754050460	0.87264
369035587	0.76141	1548456031	0.81870	1355089539	0.81664	1548456031	0.86987
-915921591	0.76105	1161743188	0.81829	676696642	0.81448	1161743188	0.86855
389713771	0.75815	629824009	0.81696	1204822525	0.81354	756894484	0.86801
233506352	0.75743	523007613	0.81676	1486464937	0.81198	323731619	0.86786
210014925	0.75671	756894484	0.81657	1423452210	0.81188	523007613	0.86782
218096097	0.75589	323731619	0.81642	1691546765	0.81183	629824009	0.86754
912589622	0.75589	908876986	0.81628	1496297303	0.81114	1919638730	0.86693
995272310	0.75568	1352158295	0.81626	351957963	0.81091	1352158295	0.86684
523007613	0.75309	1919638730	0.81611	1211893494	0.81015	908876986	0.86666
14293512	0.75282	1507196707	0.81599	942499575	0.81015	1507196707	0.86631
912296025	0.75282	660209676	0.81570	1686205177	0.81012	1049883918	0.86620
-818690456	0.75253	1049883918	0.81564	1070646765	0.81012	1033683247	0.86602
652892167	0.75199	1199232968	0.81533	1771426282	0.80990	1154335007	0.86581
187606023	0.75195	775670833	0.81478	709885352	0.80977	1199232968	0.86568
389798186	0.75118	1033683247	0.81436	1875212735	0.80943	660209676	0.86536
498302299	0.75039	1154335007	0.81397	1977654935	0.80873	775670833	0.86521

Table 2. The number of LCGs that pass the two-level statistical tests

	Runs	AR1	AR2	AR3	CS	Serial 2	Serial 3	All
$S(T, W)$	19	17	16	20	18	18	18	10
$S(T, A)$	18	18	20	19	18	18	19	14
$S(E, W)$	16	18	19	19	18	17	19	12
$S(E, A)$	18	18	20	19	18	18	19	14

four performance measures of spectral test $S(T, W)$, $S(T, A)$, $S(E, W)$, and $S(E, A)$ are proposed. For each performance measure, an exhaustive search for the best twenty full period LCGs is conducted. Results are evaluated and compared using the number of LCGs that pass all the two-level statistical tests. The number of LCGs that pass all the two-level statistical tests is affected more by the aggregation measure than that of the lower bound, indicating that it is a reason to exert more effort to use average-case performance measure. Among the average-case performance measure, the theoretical lower bound outperforms with respect to the applicability. Therefore, the spectral test with both theoretical lower bound and average-case criterion can be applied to find ideal LCGs.

Acknowledgment

The authors would like to acknowledge the anonymous

referees for their insightful comments and careful readings of the manuscript. This work was supported by the National Science Council of the Republic of China under Contract NSC-91-2416-H-151-008.

References

- [1] Lehmer, D. H., *Proceedings 2nd Symposium on Large-scale Digital Calculating Machinery*, Cambridge, Harvard University Press, pp. 141–146 (1951).
- [2] Fishman, G. S., *Monte Carlo: Concepts, Algorithms, and Applications*, Springer Series in Operations Research, Springer-Verlag, New York (1996).
- [3] Knuth, D. E., *The Art of Computer Programming, Semi-numerical Algorithms*, 2: 3rd edition, Addison-Wesley, Reading MA (1997).
- [4] Niederreiter, H., *Random number generation and quasi-Monte Carlo methods*, SIAM CBMS-NSF Re-

- gional Conference Series in Applied Mathematics*, Vol. 63, SIAM, Philadelphia (1992).
- [5] Fishman, G. S. and Moore III, L. R., "An Exhaustive Analysis of Multiplicative Congruential Random Number Generators with Modulus $2^{31} - 1$," *SIAM Journal on Scientific and Statistical Computing*, Vol. 7, pp. 24–45 (1986).
- [6] L'Ecuyer, P., Blouin, F. and Couture, R., "A Search for Good Multiple Recursive Random Number Generators," *ACM Transactions on Modeling and Computer Simulation*, Vol. 3, pp. 87–98 (1993).
- [7] Tang, H. C., "A Statistical Analysis of the Screening Measure of Multiple Recursive Random Number Generators of Orders One and Two," *Journal of Statistical Computation and Simulation*, Vol. 71, pp. 345–356 (2001).
- [8] Tang, H. C., "An Analysis of Linear Congruential Random Number Generators when Multiplier Restrictions Exist," *European Journal of Operational Research*, Vol. 182, pp. 820–828 (2007).
- [9] Coveyou, R. R. and MacPherson, R. D., "Fourier Analysis of Uniform Random Number Generators," *Journal of the ACM*, Vol. 14, pp. 100–119 (1967).
- [10] Fincke, U. and Pohst, M., "Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis," *Mathematics of Computation*, Vol. 44, pp. 463–471 (1985).
- [11] Cassels, J. W. S., *An Introduction to the Geometry of Number*, Springer-Verlag, New York (1959).
- [12] L'Ecuyer, P., "Testing Random Number Generators," *Proceeding of the 1992 Winter Simulation Conference*, pp. 305–313 (1992).

Manuscript Received: Apr. 9, 2007

Accepted: Oct. 4, 2008