Pergamon

*Computers Math. Applic.* Vol. 33, No. 4, pp. 119–125, 1997
Copyright©1997 Elsevier Science Ltd
Printed in Great Britain. All rights reserved
0898-1221/97 $17.00 + 0.00

**PII: S0898-1221(97)00012-6**

# Upper Bounds in Spectral Test for Multiple Recursive Random Number Generators with Missing Terms

CHIANG KAO* AND HUEY-CHIN TANG
Graduate School of Industrial Management, National Cheng Kung University
Tainan, Taiwan 70101, R.O.C.

*(Received April 1996; accepted May 1996)*

**Abstract**—One method for generating random numbers (RNs) of long period recommended by many scholars is the multiple recursive generator (MRG), in that the current RN is essentially a linear combination of the $k$ preceding ones. In this paper, the upper bounds for a figure of merit adopted in the spectral test are derived for the $k^{\text{th}}$ order MRG with $p \le k$ terms. As $p$ gets smaller, the bounds become smaller as well. The simplest form of the $k^{\text{th}}$ order MRG with two terms frequently discussed in literature is found to have the worst bound.

**Keywords**—Random number generator, Spectral test, Integer program.

## INTRODUCTION

The study of the methodology of generating random numbers (RNs) has a long history, in that the great majority of RN generators in use today are multiplicative linear congruential generators (MLCGs) of the form:

$$R_n = aR_{n-1} \mod m, \tag{1}$$

where $m$, $a$, and the seed $R_0$ are positive integers. When the multiplier $a$ and the modulus $m$ are chosen properly, a full period of $m-1$ can be attained. Accompanied with the rapid advances in computer technology, longer sequences of RNs become more demanding for applications. To produce RNs of longer period, one idea is to employ higher order linear recursions. This results in the class of multiple recursive generators (MRGs) [1–3]:

$$R_n = a_1R_{n-1} + \cdots + a_kR_{n-k} \mod m. \tag{2}$$

The initial values $R_0, \dots, R_{k-1}$ are not all zero. A $k^{\text{th}}$ order MRG can achieve a period length of $m^k - 1$ if and only if the polynomial

$$f(x) = x^k - a_1x^{k-1} - \cdots - a_{k-1}x - a_k, \tag{3}$$

is a primitive polynomial modulo $m$ [4]. Denoting $r = (m^k-1)/(m-1)$, Knuth [4] describes the following conditions for testing for primitivity modulo $m$:

(i) $(-1)^{k-1}a_k$ is a primitive root modulo $m$,
(ii) $[x^r \operatorname{mod} f(x)] \operatorname{mod} m = (-1)^{k-1}a_k$,
(iii) degree $\{[x^{r/s} \operatorname{mod} f(x)] \operatorname{mod} m\} > 0$ for each prime factor $s$ of $r$.

*Author to whom correspondence is to be sent.

Typeset by $\mathcal{AMS}$-TEX

Theoretically, there are exactly $\phi(m^k-1)/k$ choices of $(a_1,\dots,a_k)$ which satisfy these conditions, where $\phi(m^k-1)$ is the Euler function defined as the number of integers which is smaller than and relatively prime to $m^k-1$. For the simplest case of $k=2$ and the very popular modulus $m=2^{31}-1$, there are around 5.74E17 candidates. Hence, a significant amount of computation is involved in searching for $(a_1,\dots,a_k)$ which are able to produce RNs of full period. Nonetheless, as described in Knuth [4], "all known evidence indicates that the result will be a very satisfactory source of RN." It is therefore worthwhile to investigate the properties of the RNs produced by this type of generators.

## LATTICE STRUCTURE

Coveyou and MacPherson [5] and Marsaglia [6] find that the vectors of successive numbers produced by a linear congruential generator in any dimension have a lattice structure. Consider a sequence of full-period RNs $\{R_n, n=0,1,2,\dots\}$ produced from an MRG. Let $L_t=\{(R_n,R_{n+1},\dots,R_{n+t-1})^{\mathrm{T}}+mz \mid n\geq 0, z\in Z^t\}\cup\{0\}$ be the set of all $t$-tuples of consecutive RNs and the periodic continuations plus the zero vector. Then the set $L_t$ is called a lattice which can be expressed as:

$$L_t=\left\{R=\sum_{i=1}^{t} z_iV_i \mid z_i \text{ integer}\right\}, \tag{4}$$

where $V_i\in Z^t$ are bases of the lattice $L_t$ [7]. The dual lattice is represented by:

$$L_t^*=\left\{R^*=\sum_{i=1}^{t} z_i^*V_i^* \mid z_i^* \text{ integer}\right\}, \tag{5}$$

where $V_j^*$ is defined by $V_iV_j^*=\delta_{ij}$ [8]. The lattice structure implies that the points of $L_t$ lie in parallel hyperplanes of equal distance, and the reciprocal length of any vector in $L_t^*$ is the distance between two successive hyperplanes of order $k$ in dimension $t$. The spectral test introduced by Coveyou and MacPherson [5] essentially determines the maximum distance between adjacent hyperplanes. Most of the recommended RN generators are selected from a spectral test [9–13]. Let $d_t(k)=1/\nu_t(k)$ be the maximum distance, smaller values of $d_t(k)$ implies smaller empty slices in $L_t$ and are thus favored. Define

$$A=\begin{bmatrix} 0 & 0 & 0 & \dots & 0 & a_k \\ 1 & 0 & 0 & \dots & 0 & a_{k-1} \\ 0 & 1 & 0 & \dots & 0 & a_{k-2} \\ & \vdots & & \ddots & \vdots & \\ 0 & 0 & 0 & \dots & 1 & a_1 \end{bmatrix}, \tag{6}$$

and let $[A]_{ij}$ denote the $ij^{\text{th}}$ element of $A$. Substituting $R_{n+t-1}$ into (2) recursively derives:

$$R_{n+t-1}=[A^t]_{kk}R_{n-1}+[A^t]_{k-1,k}R_{n-2}+\cdots+[A^t]_{1k}R_{n-k} \mod m, \tag{7}$$

where $t$ in $A^t$ is the power, rather than transposition. Finding the spacing between adjacent hyperplanes in a family is equivalent to solving the following integer quadratic program:

$$\begin{aligned} \nu_t^2(k) &= \min u_1^2+u_2^2+\cdots+u_t^2, \\ \text{s.t. } u_1 & \quad +[A]_{1k}u_{k+1}+[A^2]_{1k}u_{k+2}+\cdots+[A^{t-k}]_{1k}u_t=0 \mod m, \\ u_2 & \quad +[A]_{2k}u_{k+1}+[A^2]_{2k}u_{k+2}+\cdots+[A^{t-k}]_{2k}u_t=0 \mod m, \\ & \ddots \\ & u_k+[A]_{kk}u_{k+1}+[A^2]_{kk}u_{k+2}+\cdots+[A^{t-k}]_{kk}u_t=0 \mod m, \\ & u_h\in\{-(m-1),\dots,m-1\} \text{ and not all zero.} \end{aligned} \tag{8}$$

Notice that $d_t(k) = 1/\nu_t(k)$. Since theoretical lower bound exists for $d_t(k)$ of all possible lattices with the same $L_t$, a measure suggested by Fishman and Moore [10] for comparing generators with different values of $m$ is

$$S_t(k) = \frac{d_t^*(k)}{d_t(k)}, \tag{9}$$

where $d_t^*(k)$ indicates the lower bound. In [14]:

$$d_t^*(k) = \begin{cases} \dfrac{m^{-k/t}}{r_t}, & \text{if } t > k, \\ \dfrac{1}{m}, & \text{if } t \le k, \end{cases} \tag{10}$$

and $r_t$ 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. The closer $S_{k+1}(k), S_{k+2}(k), \dots$ are to unity, the better the performance is of the corresponding MRG. Therefore, one figure of merit is

$$S_T^*(k) = \min_{k<t\le T} S_t(k), \tag{11}$$

in $k+1, \dots, T$ dimensions. In (2), computing $a_i R_{n-i} \bmod m$ accounts for most of the computation time, and the speed of a generator is approximately inversely proportional to the number of such operations [2]. Obviously, MRG with fewer terms in the recursive relationship is desired from the viewpoint of computation efficiency. The simplest MRG of order $k$ has two terms. In the section that follows, we shall derive the upper bound for $S_T^*(k)$ of this type of generators.

## TRINOMIAL CASE

When the polynomial (3) is a trinomial of the form:

$$f(x) = x^k - a_j x^{k-j} - a_k, \tag{12}$$

the corresponding MRG becomes:

$$R_n = a_j R_{n-j} + a_k R_{n-k} \mod m. \tag{13}$$

In addition to $a_k$, there is only one $a_j$, $j < k$ which is nonzero. This is the simplest MRG of order $k$. As long as the trinomial is a primitive polynomial modulo $m$, the corresponding MRG can achieve the full period of $m^k - 1$. Since the implementation of (13) requires only two multiplications modulo $m$, the efficiency in computation is conceivable. The problem is whether it possesses the desirable randomness properties. In this paper, we shall use the spectral test, the one considered by Knuth [4] as "by far the most powerful test known," to discuss the quality of the $k^{\text{th}}$ order MRG with two terms. The following proposition sets the bound for $S_T^*(k)$ in (11).

Proposition 1. *$S_T^*(k)$ of the two-term MRG is bounded by $2^{1/6} m^{-(k-2)/3(k+1)} / r_{k+1}$.*

Proof. To derive the bound for $S_T^*(k)$ it suffices to calculate $S_t(k)$ of a specific dimension, say $k+1$, because $S_T^*(k) \le S_t(k)$, $k < t \le T$. Following (8):

$$\begin{array}{llr} \nu_{k+1}^2(k) = \min u_1^2 + u_2^2 + \cdots + u_{k+1}^2, & & \\ \qquad \text{s.t. } u_1 & & + a_k u_{k+1} = 0 \mod m, \\ \qquad\qquad u_2 & & + 0 u_{k+1} = 0 \mod m, \\ \qquad\qquad\quad \ddots & & \\ \qquad\qquad\qquad u_{k-j+1} & & + a_j u_{k+1} = 0 \mod m, \\ & \ddots & \\ & u_k & + 0 u_{k+1} = 0 \mod m, \\ \qquad u_h \in \{-(m-1), \dots, m-1\} \text{ and not all zero.} & & \end{array} \tag{14}$$

To attain the minimum value of $\nu^2_{k+1}(k)$, it is obvious that $u_h = 0$, $h \neq 1$, $k-j+1$, $k+1$. Therefore, (14) is simplified to:

$$\begin{aligned} \nu^2_{k+1}(k) = \min\ & u_1^2 + u_{k-j+1}^2 + u_{k+1}^2, \\ \text{s.t. } & u_1 \qquad\quad + a_k u_{k+1} = 0 \bmod m, \\ & u_{k-j+1} + a_j u_{k+1} = 0 \bmod m, \\ & u_1, u_{k-j+1}, u_{k+1} \in \{-(m-1), \dots, m-1\} \text{ and not all zero,} \end{aligned} \tag{15}$$

which is the same as $\nu^2_3(2)$ for the second order MRG: $R_n = a_j R_{n-1} + a_k R_{n-2} \bmod m$, because

$$\begin{aligned} \nu^2_3(2) = \min\ & u_1^2 + u_2^2 + u_3^2 \\ \text{s.t. } & u_1 \quad + a_k u_3 = 0 \bmod m, \\ & u_2 + a_j u_3 = 0 \bmod m, \\ & u_1, u_2, u_3 \in \{-(m-1), \dots, m-1\} \text{ and not all zero.} \end{aligned} \tag{16}$$

Therefore, $\nu_{k+1}(k) = \nu_3(2)$. From (9) and (10),

$$S_{k+1}(k) = d^*_{k+1}(k)\nu_{k+1}(k) = \frac{\nu_{k+1}(k) m^{-k/(k+1)}}{r_{k+1}}, \tag{17}$$

$$S_3(2) = \frac{\nu_3(2) m^{-2/3}}{r_3}. \tag{18}$$

Substituting (18) into (17):

$$\begin{aligned} S_{k+1}(k) &= \frac{\nu_3(2) m^{-k/(k+1)}}{r_{k+1}} = \left[\frac{S_3(2)}{\left(m^{-2/3}/r_3\right)}\right] \frac{m^{-k/(k+1)}}{r_{k+1}} \\ &= \frac{S_3(2) m^{-(k-2)/3(k+1)} 2^{1/6}}{r_{k+1}} \leq \frac{m^{-(k-2)/3(k+1)} 2^{1/6}}{r_{k+1}}. \end{aligned} \tag{19}$$

The last step is derived from the fact that any $S_t(k)$ lies between 0 and 1. Since $S^*_T(k) \leq S_{k+1}(k)$, $S^*_T(k)$ is bounded by $2^{1/6} m^{-(k-2)/3(k+1)}/r_{k+1}$. This completes the proof. ∎

This proposition stresses that for the two-term $k^{\text{th}}$ order MRG, no matter which intermediate $a_j R_{n-j}$ term is ($j$ can be $1, 2, \dots,$ or $k-1$), the bound for $S^*_T(k)$ is the same. A careful examination of (19) also reveals that for $m$ being fixed, MRGs of higher orders have smaller bounds. For instance, $S^*_T(k)$, $k = 3, 4, 5, 6$, and 7 are bounded by 0.15749, 0.05195, 0.02422, 0.01392, and 0.00903, respectively, when $m = 2^{31} - 1$. As $k$ increases, the bound decreases.

In the proof of Proposition 1, the bound is derived from the $(k+1)^{\text{st}}$ dimension. One may suspect whether other dimensions have stronger bounds. As an empirical investigation, consider the third order MRG: $R_n = a_j R_{n-j} + a_3 R_{n-3} \bmod (2^{31} - 1)$, $j = 1$ or 2. Since an exhaustive analysis of all $(a_1, 0, a_3)$ and $(0, a_2, a_3)$ combinations is almost out of the question, we fix $a_3$ at four numbers, i.e., 742938285, 950706376, 1226874159, and 62089911, recommended by Fishman and Moore [10] for one-term MLCG and six other numbers, 1439869882, 885300443, 554271143, 588399478, 379983904, and 369035587, selected somewhat arbitrarily. An exhaustive search over all possible values of either $a_1$ or $a_2$ which are able to produce full-period RNs is conducted to find the largest value of $S^*_{T=8}(3)$. Table 1 lists $S_t(3)$, $t = 4, \dots, 8$ of the best combination in terms of $S^*_8(3)$ found for the ten values of $a_3$. All of the values shown in the last column of Table 1 are smaller than the bound of 0.15749. It is interesting to note that the minimum value $S^*_8$ of all 20 cases occurs at dimension 4, i.e., the $(k+1)^{\text{st}}$ dimension, and $S_t(3)$ of other dimensions are much larger than $S_4(3)$.

L'Ecuyer *et al.* [2] have conducted an extensive computer search for good MRGs. Some $S_{k+1}(k)$ values they found for $k = 3, 4, 5$, and 6 are 0.13778 (associated with $d_4 = 6.11801\text{E-}7$), 0.00256 ($d_5 = 1.08611\text{E-}5$), 0.00283 ($d_6 = 4.57771\text{E-}6$), and 0.00141 ($d_7 = 5.28605\text{E-}6$), respectively, for $m = 2^{31} - 1$, which are smaller than the bounds stated in Proposition 1. When all of the $k$ terms appear in the $k^{\text{th}}$ order MRG, some $S_{k+1}(k)$ values found by L'Ecuyer *et al.* [2] are 0.76551 and 0.73916 for $k = 3$ and 4, respectively. These numbers are much larger than those of the two-term MRGs.

Table 1. $S_t(3)$, $t = 4, \ldots, 8$ and $S_8^*(3)$ values of 20 two-term third order MRGs.

| $a_1$ | $a_2$ | $a_3$ | $S_4$ | $S_5$ | $S_6$ | $S_7$ | $S_8$ | $S_8^*$ |
|---|---|---|---|---|---|---|---|---|
| 823207292 | 0 | 742938285 | 0.15716 | 0.62817 | 0.62973 | 0.69029 | 0.59278 | 0.15716 |
| 0 | −894272000 | 742938285 | 0.15699 | 0.41163 | 0.66547 | 0.64110 | 0.40185 | 0.15699 |
| 803122294 | 0 | 950706376 | 0.15705 | 0.61693 | 0.73621 | 0.61856 | 0.74445 | 0.15705 |
| 0 | −803122294 | 950706376 | 0.15705 | 0.72379 | 0.43592 | 0.55371 | 0.60208 | 0.15705 |
| 702081219 | 0 | 1226874159 | 0.15672 | 0.54845 | 0.71693 | 0.68908 | 0.43936 | 0.15672 |
| 0 | 595197884 | 1226874159 | 0.15703 | 0.69138 | 0.63503 | 0.59301 | 0.46911 | 0.15703 |
| 208031319 | 0 | 62089911 | 0.15673 | 0.42126 | 0.70575 | 0.57897 | 0.57826 | 0.15673 |
| 0 | −465275168 | 62089911 | 0.15670 | 0.58331 | 0.69480 | 0.44264 | 0.56597 | 0.15670 |
| 510414496 | 0 | 1439869882 | 0.15694 | 0.60624 | 0.67039 | 0.62765 | 0.58455 | 0.15694 |
| 0 | 510414496 | 1439869882 | 0.15694 | 0.48930 | 0.60816 | 0.46825 | 0.70281 | 0.15694 |
| 875179813 | 0 | 885300443 | 0.15688 | 0.46562 | 0.58157 | 0.78133 | 0.64758 | 0.15688 |
| 0 | −501972935 | 885300443 | 0.15665 | 0.69094 | 0.71528 | 0.63051 | 0.61454 | 0.15665 |
| −435715484 | 0 | 554271143 | 0.15669 | 0.39625 | 0.46244 | 0.66876 | 0.62337 | 0.15669 |
| 0 | 1009929446 | 554271143 | 0.15691 | 0.67317 | 0.77278 | 0.63981 | 0.67953 | 0.15691 |
| 706202084 | 0 | 588399478 | 0.15686 | 0.51943 | 0.76794 | 0.53748 | 0.64286 | 0.15686 |
| 0 | −706202084 | 588399478 | 0.15686 | 0.35974 | 0.34468 | 0.42035 | 0.51578 | 0.15686 |
| 874894320 | 0 | 379983904 | 0.15694 | 0.82986 | 0.58026 | 0.71835 | 0.43814 | 0.15694 |
| 0 | −821777664 | 379983904 | 0.15673 | 0.66252 | 0.70153 | 0.66695 | 0.75406 | 0.15673 |
| 150483787 | 0 | 369035587 | 0.15663 | 0.83305 | 0.70331 | 0.44516 | 0.72034 | 0.15663 |
| 0 | −192414791 | 369035587 | 0.15687 | 0.72555 | 0.66304 | 0.48831 | 0.64363 | 0.15687 |

## GENERAL CASE

Consider a more complicated case of the $k^{\text{th}}$ order MRG with three terms:

$$R_n = a_i R_{n-i} + a_j R_{n-j} + a_k R_{n-k} \mod m. \tag{20}$$

The bounds for $S_T^*(k)$ of different $m$ and $k$ can be derived similarly.

PROPOSITION 2. *$S_T^*(k)$ of the three-term MRG is bounded by $2^{1/4} m^{-(k-3)/4(k+1)} / r_{k+1}$.*

PROOF. Following (8), $\nu_{k+1}^2(k)$ for the MRG (20) can be solved from the following integer program:

$$\begin{array}{llllllr}
\nu_{k+1}^2(k) = \min u_1^2 + u_2^2 + \cdots + u_{k+1}^2, & & & & & & \\
\qquad \text{s.t. } u_1 & & & & & & + a_k u_{k+1} = 0 \mod m, \\
 & u_2 & & & & & + 0 u_{k+1} = 0 \mod m, \\
 & & \ddots & & & & \\
 & & & u_{k-j+1} & & & + a_j u_{k+1} = 0 \mod m, \\
 & & & & \ddots & & \\
 & & & & & u_{k-i+1} & + a_i u_{k+1} = 0 \mod m, \\
 & & & & & & \ddots \\
 & & & & & & u_k + 0 u_{k+1} = 0 \mod m, \\
\qquad u_h \in \{-(m-1), \ldots, m-1\} \text{ and not all zero.} & & & & & &
\end{array} \tag{21}$$

This program is equivalent to:

$$\begin{array}{l}
\nu_{k+1}^2(k) = \min u_1^2 + u_{k-j+1}^2 + u_{k-i+1}^2 + u_{k+1}^2, \\
\qquad \text{s.t. } u_1 \qquad\qquad\qquad + a_k u_{k+1} = 0 \mod m, \\
\qquad\qquad u_{k-j+1} \qquad\quad + a_j u_{k+1} = 0 \mod m, \\
\qquad\qquad\qquad u_{k-i+1} + a_i u_{k+1} = 0 \mod m, \\
\qquad u_1, u_{k-j+1}, u_{k-i+1}, u_{k+1} \in \{-(m-1), \ldots, m-1\}, \\
\qquad u_h = 0,\ h \neq 1,\ k-j+1, k-i+1, k+1; u_h \text{ not all zero.}
\end{array} \tag{22}$$

This program has the same form as that of $\nu_4^2(3)$ for the third order MRG: $R_n = a_i R_{n-1} + a_j R_{n-2} + a_k R_{n-3} \bmod m$. Therefore, $\nu_{k+1}(k) = \nu_4(3)$. Substituting this result into (9):

$$\begin{aligned} S_{k+1}(k) &= \frac{\nu_{k+1}(k) m^{-k/(k+1)}}{r_{k+1}} = \frac{\nu_4(3) m^{-k/(k+1)}}{r_{k+1}} \\ &= \left[\frac{S_4(3)}{\left(m^{-3/4}/2^{1/4}\right)}\right] \frac{m^{-k/(k+1)}}{r_{k+1}} = \frac{S_4(3) m^{-(k-3)/4(k+1)} 2^{1/4}}{r_{k+1}} \\ &\leq \frac{m^{-(k-3)/4(k+1)} 2^{1/4}}{r_{k+1}}. \end{aligned} \tag{23}$$

Since $S_T^*(k) \leq S_{k+1}(k)$, $S_T^*(k)$ is bounded by $2^{1/4} m^{-(k-3)/4(k+1)}/r_{k+1}$. ▮

For $m = 2^{31} - 1$, the bounds are 0.32988, 0.15376, 0.08839, and 0.05731 for $k = 4, 5, 6$, and 7, respectively. Comparing the bound of two-term MRG with that of three-term MRG, we have:

$$\frac{\left[2^{1/4} m^{-(k-3)/4(k+1)}/r_{k+1}\right]}{\left[2^{1/6} m^{-(k-2)/3(k+1)}/r_{k+1}\right]} = 2^{1/12} m^{1/12}. \tag{24}$$

That is, adding one term to the two-term MRG, the bound for $S_T^*(k)$ increases by a factor of $2^{1/12} m^{1/12}$. Note that this factor is independent of $k$. For $m = 2^{31} - 1$, this factor is around 6.3496. As an empirical verification, the bounds for $k = 4, 5, 6$, and 7 for the three-term MRG, i.e., 0.32988, 0.15376, 0.08839, and 0.05731 are 6.3496 times of 0.05195, 0.02422, 0.01392, and 0.00903, respectively, which are the bounds for the two-term MRGs.

The whole concept can be extended to the $k^{\text{th}}$ order MRG with more than four terms. For the general case of $p$ terms in the $k^{\text{th}}$ order MRG, the following theorem sets the bound for $S_T^*(k)$.

THEOREM. *The $S_T^*(k)$ value of the $k^{th}$ order MRG with $p \leq k$ terms is bounded by $[r_{p+1}/r_{k+1}] \times m^{-(k-p)/(p+1)(k+1)}$.*

PROOF. Following the argument of Propositions 1 and 2, we have $\nu_{k+1}(k)$ of the $p$-term $k^{\text{th}}$ order MRG equal to $\nu_{p+1}(p)$ of the $p$-term $p^{\text{th}}$ order MRG. Consequently,

$$\begin{aligned} S_{k+1}(k) &= d_{k+1}^*(k) \nu_{k+1}(k) = \left[\frac{m^{-k/(k+1)}}{r_{k+1}}\right] \left[\frac{S_{p+1}(p) r_{p+1}}{m^{-p/(p+1)}}\right] \\ &\leq \frac{m^{-(k-p)/(p+1)(k+1)} r_{p+1}}{r_{k+1}}, \end{aligned} \tag{25}$$

which is the bound of $S_T^*(k)$. ▮

The largest value of this bound is 1 which occurs at $p = k$ when none of the $k$ terms in the $k^{\text{th}}$ order MRG vanishes. For the $k^{\text{th}}$ order MRGs with $p$ and $q > p$ terms, respectively, the ratio of their bounds for $S_T^*(k)$ is:

$$\frac{\left[m^{-(k-q)/(q+1)(k+1)} r_{q+1}/r_{k+1}\right]}{\left[m^{-(k-p)/(p+1)(k+1)} r_{p+1}/r_{k+1}\right]} = \left(\frac{r_{q+1}}{r_{p+1}}\right) m^{(q-p)/(p+1)(q+1)}, \tag{26}$$

which is greater than 1 because $r_{q+1} > r_{p+1}$ and the exponent of $m$ is positive. As more terms are included in the recursive relationship, the bound for $S_T^*(k)$ increases. Interestingly, this ratio only depends on the number of terms included in the recursive relationship and is irrelevant to the order of the generator. Moreover, the larger the modulus $m$ is, the larger this ratio will be.

## CONCLUSION

To generate RNs of long period, one method recommended by many scholars is the multiple recursive generator which is essentially the extension of the usual prime modulus MLCG from one term to $k$ terms. When the multipliers $(a_1, \ldots, a_k)$ are chosen properly, the period achieves $m^k - 1$. Since there is a trade off in the increasing of computational effort, fewer terms in the recursive formula are preferred. In this paper, it is derived that $S_T^*(k)$, a figure of merit frequently adopted in the spectral test, is bounded by $m^{-(k-p)/(p+1)(k+1)} r_{p+1}/r_{k+1}$ for the $k^{\text{th}}$ order MRG with $p$ terms. Fixing $k$, smaller $p$ has smaller bound. The most computationally efficient form of the $k^{\text{th}}$ order MRG with two terms has the worst bound. If the number of terms in the $k^{\text{th}}$ order MRG is reduced from $q$ to $p < q$, the bound for the corresponding MRG decreases by a factor of $(r_{q+1}/r_{p+1})m^{(q-p)/(p+1)(q+1)}$, which is independent of the order $k$. The larger the difference between $p$ and $q$ is, the larger the factor will be.

## REFERENCES

1. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, (1992).
2. P. L'Ecuyer, F. Blouin and R. Couture, A search for good multiple recursive random number generators, *ACM Trans. on Modeling and Computer Simu.* **3**, 87–98 (1993).
3. C. Kao and H.C. Tang, Symmetry property of multiplicative congruential random number generator in chi-square test, *Intern. J. Computer Math.* **55**, 113–118 (1995).
4. D.E. Knuth, *The Art of Computer Programming, Vol. 2: Semi-Numerical Algorithms*, 2nd ed., Addison-Wesley, Reading, MA, (1981).
5. R.R. Coveyou and R.D. MacPherson, Fourier analysis of uniform random number generators, *J. of the ACM* **14**, 100–119 (1967).
6. G. Marsaglia, Random numbers fall mainly in the planes, *Proc. of the Nat. Acad. Sci.* **60**, 25–28 (1968).
7. L. Afflerbach and H. Grothe, Calculation of Minkowski-reduced lattice bases, *Computing* **35**, 269–276 (1985).
8. U. Dieter, How to calculate shortest vectors in a lattice, *Math. Comput.* **29**, 827–833 (1975).
9. G.S. Fishman, Multiplicative congruential random number generators with modulus $2^\beta$: An exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$, *Math. Comput.* **54**, 331–344 (1990).
10. G.S. Fishman and L.R. Moore, III, An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$, *SIAM J. on Sci. Stat. Comput.* **7**, 24–45 (1986).
11. C. Kao and J.Y. Wong, Several extensively tested random number generators, *Computers Ops. Res.* **21**, 1035–1039 (1994).
12. C. Kao and J.Y. Wong, An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus smaller than $2^{15}$, *J. Statist. Comput. Simu.* **54**, 29–35 (1996).
13. S.K. Park and K.W. Miller, Random number generators: Good ones are hard to find, *Commun. of the ACM* **31**, 1192–1201 (1988).
14. J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, New York, (1959).