Version: December 16, 1996
To appear in: *INFORMS J. on Computing,* **9** *(1), Winter 1997*

Bad Lattice Structures for Vectors of Non-Successive Values Produced by Some Linear Recurrences

PIERRE L'ECUYER
Université de Montréal

ABSTRACT: Usually, the t-dimensional spectral test for linear congruential generators examines the lattice structure of all the points formed by taking t successive values in the sequence. In this paper, we consider the case where the t values taken are not successive, but separated by lags that are chosen a priori. For certain classes of linear congruential and multiple recursive generators, and for certain choices of the lags, we give lower bounds on the distance between hyperplanes. In some cases, those lower bounds are quite large, even in dimensions as small as $t = 3$. We give illustrations with specific classes of generators that have been proposed in the literature, and discuss the possible implications.

Additional Key Words and Phrases: Random Number Generation; Linear Congruential Generators; Lattice Structure; Spectral Test

---

Author's Address:
P. L'Ecuyer, Département d'Informatique et de Recherche Opérationnelle (IRO), Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal, H3C 3J7, Canada; e-mail: `lecuyer@iro.umontreal.ca`

Introduction

We consider a multiple recursive random number generator (MRG), defined by the recurrence:

$$\begin{aligned} x_n &= (a_1 x_{n-1} + \cdots + a_k x_{n-k}) \bmod m; \\ u_n &= x_n/m, \end{aligned} \tag{1}$$

where m and k are positive integers and each a_i belongs to $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$. Under appropriate conditions on m, k, and the a_i (see [5, 6, 8, 9]), the sequence $\{u_n,\ n \geq 0\}$ could be a reasonably good imitation of a sequence of independent and identically distributed (i.i.d.) uniform random variables over the interval $[0, 1]$.

For any $t > 1$ and any set of t (fixed) non-negative integers $I = \{i_1, i_2, \cdots, i_t\}$, define

$$T_t(I) = \{(u_{i_1+n}, \ldots, u_{i_t+n}) \mid n \geq 0,\ s_0 = (x_0, \ldots, x_{k-1}) \in \mathbf{Z}_m^k\} \tag{2}$$

and let $L_t(I)$ be the integer lattice generated by $T_t(I)$ and $\frac{1}{m}\mathbf{Z}_m^k$, that is, the set of all linear combinations of elements of T_t and $\frac{1}{m}\mathbf{Z}_m^k$, with integer coefficients. It is well known that the points of $L_t(I)$ lie in a set of equidistant parallel hyperplanes in the t-dimensional unit hypercube. In the context of random number generation, one would like that the distance $d_t(I)$ between those hyperplanes be relatively small, in order to avoid large slices of empty space. Traditionally, computing $d_t(I)$ has been called the *spectral test*, with the set I usually comprised of successive indices: $i_j = j$ for all j; this is the *classical* spectral test [5]. The construction (2) is more general, in the sense that the vectors of $T_t(I)$ are constructed with values that can be some distance apart in the sequence. For that reason, we call I the set of *lacunary indices*.

In this paper, we examine the behavior of $d_t(I)$ for special classes of MRGs. For some of those classes and small values of t, we obtain a fairly large lower bound on $d_t(I)$ for certain sets I. In Section 2, we briefly explain how to construct a lattice basis for $L_t(I)$, as well as for its dual. In Section 3, we look at special cases, namely the case where the number of non-zero coefficients in (1) is less than k, and the case where those coefficients are small. We derive lower bounds on $d_t(I)$. These bounds explain in particular some empirical results obtained in [9] and imply further limitations for the class of generators proposed there. Specific numerical examples are given. In Section 4, we examine a class of linear congruential generators (with $k = 1$), for which the modulus m can be expressed as a linear combination of powers of the multiplier a, with small coefficients. Again, we derive lower bounds on $d_t(I)$ for certain sets I and give illustrations using linear congruential generators which approximate the add-with-carry and subtract-with-borrow (AWC/SWB) generators. It turns out that for those generators, as well as for the lagged-Fibonacci generators, the set $T_3(I)$, for a certain set I, is contained in only two planes in the three-dimensional space. Such serious structural limitations will obviously show up in empirical statistical tests when the parameters of the tests are chosen accordingly. Finally, we examine two combined generators proposed in [14, 15] and which can be approximated by linear congruential generators for which $d_6(I) \geq 1/\sqrt{6} \approx 0.408$ for certain sets I. The lattice structure for most of the examples we consider here was already analyzed in previous papers [1, 2, 9, 17], but only for the case of successive indices. When considering lacunary indices, we obtain bad stuctures in much smaller dimensions.

It is not clear how those properties really affect the results of typical simulations in practice. Perhaps for most real-life simulations (e.g., when simulating a factory, or a restaurant, or a communication network), the results will not be affected, because the model will typically not be synchronized with the bad set of lags I (unless we are very unlucky). But that could happen, and if it does, disaster will strike. There are also classes of applications dealing specifically with random points in high dimensional space, and where those bad structures could have a dramatic effect. Such applications arise, for example, in computational physics [3], or in statistics, when estimating complicated (perhaps multidimensional) distributions or expectations by simulation [7].

1. Lattice bases and spectral test

Let $e_{i(t)}$ denote the i-th unit vector in dimension t and let $\{x_{i,n},\ n \geq 0\}$ denote the sequence obtained from (1) when $s_0 = (x_0, \ldots, x_{k-1}) = e_{i(k)}$. Consider the set of vectors $U_i = (x_{i,i_1}, \ldots x_{i,i_t})/m$, for $i = 1, \ldots, k$, together with the vectors $U_{k+i} = e_{i(t)}$ for $i = 1, \ldots, t$. These $k + t$ vectors generate $L_t(I)$ and one can construct a basis $\{V_1, \ldots, V_t\}$ of $L_t(I)$ by constructing t linearly independent vectors from the linear combinations of elements of that set (see [10] for further details). The dual basis is defined as the set of vectors $W_1, \ldots, W_t$ such that their scalar products with the V_i's satisfy $W_j' V_i = \delta_{ij}$ for all i and j, where δ_{ij} denotes the Kronecker's delta. The vectors $W_1, \ldots, W_t$ form a basis of the dual lattice $L_t^*(I)$ and the distance $d_t(I)$ is equal to one over the length of the shortest non-zero vector in $L_t^*(I)$, i.e.

$$\frac{1}{d_t(I)} = \min \left\{ \|W\| \ \mid \ W = \sum_{i=1}^{t} z_i W_i,\ z_i \in \mathbf{Z},\ \sum_{i=1}^{t} |z_i| > 0 \right\}, \tag{3}$$

where $\|\cdot\|$ denotes the Euclidean norm (see [5]).

2. Lower Bounds on $d_t(I)$ for MRGs

In this section, we shall assume that $t \leq k+1$ and that the set I of lacunary indices satisfies $0 = i_1 < i_2 < \cdots < i_t = k$. In that case, the generating set $U_1, \ldots, U_{k+1}$ is given by

$$\begin{aligned}
U_1 &= \frac{1}{m}(1, 0, \ldots, 0, a_k), \\
U_{i_2+1} &= \frac{1}{m}(0, 1, \ldots, 0, a_{k-i_2}), \\
&\vdots \\
U_{i_{t-1}+1} &= \frac{1}{m}(0, 0, \ldots, 1, a_{k-i_{t-1}}),
\end{aligned}$$

$$
\begin{aligned}
U_{k+1} &= (0,0,\ldots,0,1), \\
U_i &= \frac{1}{m}(0,0,\ldots,0,a_{k-i+1}) \qquad \text{for } i \le k \text{ and } i \notin I.
\end{aligned}
$$

From that, we obtain the basis $V_1,\ldots,V_t$, where $V_j = U_{i_j+1}$ for $j = 1,\ldots,t-1$ and $V_t = (0,\ldots,0,b)$, where $b = \gcd(m, \{a_{k-i+1} \mid 2 \le i \le k,\ i \notin I,\ a_{k-i+1} \ne 0\})$. The dual basis is given by $W_i = m\, e_{i(t)}$ for $i = 1,\ldots,t-1$, and $W_t = (m/b)(-a_k, -a_{k-i_2},\ldots,-a_{k-i_{t-1}},1)$. So, we readily obtain the following lemma:

Proposition **1.** *One has*

$$
d_t(I) \;\ge\; \frac{b}{m}\left(1+\sum_{j=1}^{t-1} a_{k-i_j}^2\right)^{-1/2}.
$$

Proof. From (3), it is clear that $1/d_t(I) \le \|W_t\|$. But the Euclidean norm of W_t is given by

$$
\|W_t\| = \frac{m}{b}\left(1+\sum_{j=1}^{t-1} a_{k-i_j}^2\right)^{1/2}.
$$

From that, the inequality follows easily. □

As a special case, suppose that I contains all the indices i such that $a_{k-i+1} \ne 0$. Then, one has $b = m$ and Proposition 1 reduces to:

Proposition **2.** *If $i \notin I$ implies $a_{k-i+1} = 0$, then*

$$
d_t(I) \;\ge\; \left(1+\sum_{i=1}^{k} a_i^2\right)^{-1/2}.
$$

As a further special case, suppose that the recurrence has only two non-zero coefficients, say a_r and a_k, as suggested in [9] (i.e., its characteristic polynomial is a trinomial of the form $f(x) = x^k - a_r x^{k-r} - a_k$). Let $t = 3$. If $k \ge 3$ and $0 = i_1 < i_2 < k$, then $d_3(I) = 1/m$. But if $I = \{0, k-r, k\}$, then $\|W_3\|^2 = (1 + a_r^2 + a_k^2)$ and

$$
\begin{aligned}
d_3(I) &\ge (1 + a_r^2 + a_k^2)^{-1/2} && (4)\\
&\ge (1 + 2(m-1)^2)^{-1/2} \\
&> 1/(m\sqrt{2}). && (5)
\end{aligned}
$$

The lower bound (4) is especially bad when the non-zero coefficients a_k and a_r are small. For example, if we assume that each $|a_i|$ is smaller than $\sqrt{m}$, as is sometimes suggested to facilitate the implementation [6], then

$$
d_3(I) \;\ge\; (1 + 2(m-1))^{-1/2} \;>\; 1/\sqrt{2m}. \tag{6}
$$

Example 1. Let $m = 2^{31} - 1$. Suppose that the recurrence has only two non-zero coefficients a_r and a_k, with $k \geq 3$, and let $t = 3$. If $I = \{0, 1, 2\}$, then $d_3(I) = 1/m \approx 4.6566 \times 10^{-10}$. If $I = \{0, k - r, k\}$, then $d_3(I) > 1/(m\sqrt{2}) \approx 3.2927 \times 10^{-10}$, which is still good. However, if $|a_k|$ and $|a_r|$ are less than $\sqrt{m}$, then (6) gives $d_3(I) \geq 1.5259 \times 10^{-5}$. That explains the small values of d_t and q_t obtained in [9] for $t > k$ when the coefficients satisfied those conditions.

Example 2. Consider an additive or subtractive lagged-Fibonacci generator, with modulus m and lags $0 < r < k$:

$$\begin{aligned} x_n &= (\pm x_{n-r} \pm x_{n-k}) \bmod m; \\ u_n &= x_n/m. \end{aligned} \tag{7}$$

In that case, if $t = 3$ and $I = \{0, k-r, k\}$, then (4) gives $d_3(I) \geq 1/\sqrt{3}$, whatever be the values of m and k. Therefore, all the three-dimensional points $(u_n, u_{n+k-r}, u_{n+k})$ produced by such a generator lie in parallel planes that are at least $1/\sqrt{3}$ apart. In fact, a closer examination shows that all those points lie in only two parallel planes which are perpendicular to the vector $(1, 1, -1)$, one of them passing through the origin and the other one passing through the point $(1/2, 1/2, 0)$. So, this class of generators has an extremely bad lattice structure for those lacunary indices. The lower bound of $1/\sqrt{3}$ for $d_t(I)$ also stands for any I that contains the indices $\{0, k - r, k\}$, for $t > 3$.

Several instances of lagged-Fibonacci generators have been recommended in the literature for $m = 2^e$, where e is often taken equal to 24, because then the generator can be implemented directly in "standard" floating-point arithmetic. This yields extremely fast generators. For example, Mitchell and Moore devised in 1958 a generator based on the recurrence

$$x_n = (x_{n-24} + x_{n-55}) \bmod 2^e.$$

This generator is proposed and described in Knuth [5, pp.26–27]. Knuth said that it "may well prove to be the very best source of random numbers for practical purposes", but also admitted that it was difficult to "recommend it wholeheartedly", because there was "still very little theory to prove that it does or does not have desirable randomness properties". The generator *addrans* provided by the mathematical library libm.a of the SunOS operating system [16, Chap. 4] is a slight variant of that same generator: the plus sign has just been replaced by a minus sign. Another example is the generator based on

$$x_n = (x_{n-5} + x_{n-17}) \bmod 2^{24},$$

suggested by Marsaglia [12]. It follows from our results that these generators have highly unfavorable properties and should be avoided.

3. A Bound on $d_t(I)$ for certain Linear Congruential Generators

Consider now a linear congruential generator (LCG):

$$x_n = a x_{n-1} \bmod m,$$

again with $u_n = x_n/m$. In that case, a basis for $L_t(I)$ is given by $V_1 = \frac{1}{m}(1, a^{i_2}, \ldots, a^{i_t})$ and $V_i = e_{i(t)}$ for $i = 2, \ldots, t$. The dual basis is given by $W_1 = me_{1(t)}$ and $W_j = me_{j(t)} - a^{i_j} e_{1(t)}$ for $j = 2, \ldots, t$.

Proposition **3.** *Suppose that the modulus m can be expressed as*

$$m = \sum_{j=1}^{t} c_{i_j} a^{i_j}$$

for some integers c_ℓ, $\ell \in I$. Then,

$$d_t(I) \geq \left(\sum_{j=1}^{t} c_{i_j}^2 \right)^{-1/2}.$$

Proof. Consider the vector

$$W = W_1 + \sum_{j=2}^{t} c_{i_j} W_j = (c_0, c_{i_2}, \ldots, c_{i_t}).$$

This vector belongs to the dual lattice and its square length is $\|W\|^2 = \sum_{j=1}^{t} c_{i_j}^2$. The result follows. □

A class of add-with-carry and subtract-with-borrow (AWC/SWB) generators has been proposed by Marsaglia and Zaman [13] and studied further in [1, 17]. These generators turn out to be practically equivalent to LCGs with multiplier a and modulus $m = a^k \pm a^r \pm 1$. More precisely, the absolute difference between the u_n produced by the approximating LCG and that produced by the AWC/SWB generator is bounded by $1/a$. But it follows from the proposition that the three-dimensional vectors (u_n, u_{n+r}, u_{n+k}) produced by those LCGs lie in parallel planes that are at least $1/\sqrt{3}$ apart, as was the case in Example 2. It was already shown in [1] that the t-dimensional vectors of successive values produced by the approximating LCG lie in parallel hyperplanes which are exactly $1/\sqrt{3}$ apart for $k \leq t \leq t^*$ for some t^* (and $1/\sqrt{2}$ apart thereafter). When m is prime, t^* is the least integer f such that $a^f \equiv \pm 1 \pmod{m}$. Combined with our Proposition 3, this implies that $d_t(I) = 1/\sqrt{3}$ whenever I contains $\{0, r, k\}$ and $i_t \leq t_*$.

Example **3.** One SWB generator recommended in [4] has $k = 24$, $r = 10$, $a = 2^{24}$, and $m = a^{24} - a^{10} + 1$. The vectors $(u_n, u_{n+10}, u_{n+24})$ produced by that generator lie within a distance of 2^{-24} to a pair of planes which are $1/\sqrt{3}$ apart. This highly unfavorable structure can be detected by simple empirical statistical tests such as the serial test in three dimensions [5, p.60], provided that we choose the appropriate (non-successive) dimensions.

If we combine a AWC/SWB generator which is equivalent to a LCG with modulus $m_1 = a^k \pm a^r \pm 1$ with, say, a LCG with modulus m_2, by adding or subtracting their states, then the combined generator is often well approximated by a LCG with modulus $m = m_1 m_2$ [1].

Typically, the bound given by Proposition 3 is not very useful in that case, but other results proved in [1] can be used to obtain a short vector in the dual lattice, as illustrated by the next example. Other related techniques developed in [2] can also be used to find a short vector in the dual lattice associated with certain classes of combined LCGs; our last example gives an illustration of how this may sometimes provide us with a bad set I of lacunary indices.

Example **4.** Marsaglia, Narasimhan, and Zaman [14] have proposed a combined generator whose first component is the SWB with $k = 43$, $r = 22$, $a = a_1 = 2^{32} - 5$, and $m = m_1 = a_1^{43} - a_1^{22} + 1$, whereas the second component is a LCG based on the recurrence $z_{n+1} = (z_n + 362436069) \bmod 2^{32}$. The combination is defined by subtracting the state of the LCG from that of the SWB, modulo $m_2 = 2^{32}$, and then dividing by 2^{32}. As shown in [1], that generator can be approximated by a LCG with modulus $m = m_1 m_2 = 2^{32}(a^{43} - a^{22} + 1)$ and multiplier a such that $a \bmod m_1 = a_1$ and $a \bmod m_2 = a_2 = 1$, with a difference of at most 6×2^{-32} on the values of u_n. From the results of Table 1 in [1], one can also easily deduce that in dimension 45, a shortest vector is $W = e_{44(45)} - e_{23(45)} + e_{1(45)} - (e_{45(45)} - e_{24(45)} + e_{2(45)})$. It follows that in dimension $t = 6$, by choosing $I = \{0, 1, 22, 23, 43, 44\}$, one obtains a vector of square length 6 in the dual basis. Then, $d_6(I) \geq 1/\sqrt{6} \approx 0.408$. It is relatively easy to design empirical statistical tests in 6 dimensions that will detect that structure.

Example **5.** Marsaglia, Zaman, and Tsang [15] proposed a combined generator now widely available and known under the name of RANMAR. James [4] gives a FORTRAN implementation. It is based on the recurrences

$$
\begin{aligned}
y_n &= (y_{n-97} - y_{n-33}) \bmod 2^{24} \\
z_n &= (z_{n-1} - 7654321) \bmod (2^{24} - 3) \\
x_n &= (y_n - z_n) \bmod 2^{24},
\end{aligned}
$$

and the output at step n is $u_n = 2^{-24} x_n$. It can be verified [2] that this generator can be closely approximated (one has $|\tilde{x}_n - x_n| \leq 3 \times 2^{-24}$) by the MRG based on the recurrence:

$$
\begin{aligned}
\tilde{x}_n = \; & (187649956511744\tilde{x}_{n-1} + 187649956511743\tilde{x}_{n-33} \\
& +93824969867265\tilde{x}_{n-97} - 7654321) \bmod (2^{24}(2^{24} - 3)).
\end{aligned}
$$

The latter MRG has main subcycles of length 2^{144} (much less than the size of its state space, which is near 2^{4656}). It turns out that the lattice generated by each of the main subcycles is a strict sublattice of that generated by the full state space. Those sublattices are analyzed in [2]. In particular, in dimension 99, the following vector belongs to the dual basis: $W = e_{99(99)} - e_{98(99)} + e_{66(99)} - e_{65(99)} - e_{2(99)} + e_{1(99)}$. It follows that in dimension $t = 6$, by choosing $I = \{0, 1, 64, 65, 97, 98\}$, one obtains (again) $d_6(I) \geq 1/\sqrt{6}$.

It might be interesting to observe that if the modulus $2^{24} - 3$ in the recurrence for z_n would have been 2^{24} instead, then x_n would follow exactly the recurrence:

$$x_n = (-x_{n-98} + x_{n-97} + x_{n-34} - x_{n-33} + x_{n-1} + 7654321) \bmod 2^{24}.$$

It is well known that the structure of the lattice $L_t(I)$ associated with such a recurrence does not depend on the constant term 7654321; that constant just shifts the lattice [5]. Therefore, it would then follow from Proposition 2 that $d_t(I) \geq 1/\sqrt{6}$ for (once again) $t = 6$ and $I = \{0, 1, 64, 65, 97, 98\}$.

Acknowledgments

This work has been supported by NSERC-Canada grant # ODGP0110050 and FCAR-Québec grant # 93ER1654. I wish to thank Raymond Couture, W. David Kelton, and the referees for their helpful comments.

References

[1] R. Couture and P. L'Ecuyer, 1994. On the Lattice Structure of Certain Linear Congruential Sequences Related to AWC/SWB Generators, *Mathematics of Computation 62*, 798–808.

[2] R. Couture and P. L'Ecuyer, 1996. Orbits and Lattices for Linear Random Number Generators with Composite Moduli, *Mathematics of Computation 65*, 189–201.

[3] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, 1992. Monte Carlo Simulations: Hidden Errors from "Good" Random Number Generators, *Physical Review Letters 69*, 23, 3382–3384.

[4] F. James, 1990. A review of pseudorandom number generators, *Computer Physics Communications 60*, 329-344.

[5] D. E. Knuth, 1981. *The Art of Computer Programming : Seminumerical Algorithms*, vol. 2, second edition. Addison-Wesley, Reading, Mass.

[6] P. L'Ecuyer, 1990. Random Numbers for Simulation, *Communications of the ACM 33, 10*, 85–97.

[7] P. L'Ecuyer, 1992. Testing Random Number Generators, *Proceedings of the 1992 Winter Simulation Conference* (Arlington, Virginia), IEEE Press, Pistacaway, N.J., 305–313.

[8] P. L'Ecuyer, 1994. Uniform Random Number Generation, *Annals of Operations Research 53*, 77–120.

[9] P. L'Ecuyer, F. Blouin, and R. Couture, 1993. A Search for Good Multiple Recursive Generators, *ACM Transactions on Modeling and Computer Simulation 3*, 87–98.

[10] P. L'Ecuyer and R. Couture, 1997. An Implementation of the Lattice and Spectral Tests for Multiple Recursive Linear Random Number Generators, *INFORMS Journal on Computing*, to appear.

[11] P. L'Ecuyer and S. Tezuka, 1991. Structural Properties for Two Classes of Combined Random Number Generators. *Mathematics of Computation 57*, 735–746.

[12] G. Marsaglia, 1985. A Current View of Random Number Generation, *Computer Science and Statistics, Proceedings of the Sixteenth Symposium on the Interface*, Elsevier Science Publ. (North-Holland), 3–10.

[13] G. Marsaglia and A. Zaman, 1991. A New Class of Random Number Generators, *The Annals of Applied Probability 1*, 462–480.

[14] G. Marsaglia, B. Narasimhan, and A. Zaman, 1990. A Random Number Generator for PC's, *Computer Physics Communications 60*, 345–349.

[15] G. Marsaglia, A. Zaman, and W. W. Tsang, 1990. Towards a Universal Random Number Generator, *Stat. and Prob. Letters 8*, 35–39.

[16] Sun Microsystems, 1991. *Numerical Computations Guide*, Document number 800-5277-10.

[17] S. Tezuka, P. L'Ecuyer, and R. Couture, 1993. On the Lattice Structure of the Add-with-Carry and Subtract-with-Borrow Random Number Generators, *ACM Transactions of Modeling and Computer Simulation 3*, 315–331.