

On the Lattice Structure of a Special Class of Multiple Recursive Random Number Generators

Pierre L'Ecuyer, Richard Simard

Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Montréal, Québec H3C 3J7, Canada
 {lecuyer@iro.umontreal.ca, simardr@iro.umontreal.ca}

We examine some properties of the points produced by certain classes of long-period linear multiple recursive random number generators proposed by L.-Y. Deng and his co-authors in several papers. These generators have their parameters selected in special ways to make the implementation faster. We show that as a result, the points produced by these generators have a poor lattice structure, and a poor initialization of the state can have long-lasting impact, because of the limited diffusion capacity of the recurrence.

Keywords: random number generators; multiple recursive generators; lattice structure; simulation

History: Accepted by David Woodruff, EIC and (former) Area Editor for Heuristic Search and Learning; received May 2013; accepted July 2013. Published online in *Articles in Advance*.

1. Introduction

A widely used type of uniform random number generator for simulation, known as *multiple recursive generators* (MRG), is based on a linear recurrence of the form

$$x_i = (a_1 x_{i-1} + \dots + a_k x_{i-k}) \bmod m, \quad (1)$$

$$u_i = x_i / m, \quad (2)$$

where m (the modulus) and k (the order) are positive integers, the a_j (the coefficients) are in $\{0, 1, \dots, m-1\}$, and $u_i \in [0, 1)$ is the output (or random number generated) at step i . Typically, m is a prime number and the coefficients a_j are selected so that the characteristic polynomial of the recurrence (1) is a primitive polynomial, in which case the output sequence is periodic with (maximal) period $\rho = m^k - 1$ (Knuth 1998). In practice, the output u_i is often modified slightly (e.g., by adding $0.5/m$) to avoid returning zero, but this has little impact on the analysis and we ignore it here for simplicity. More details on the MRG and its properties can be found in L'Ecuyer (1999a, 2006) and Niederreiter (1992), for example.

In a series of papers, L.-Y. Deng and his co-authors have proposed various special cases of MRGs of large order k , where the coefficients a_j satisfy certain conditions that can make the implementation faster (Deng and Lin 2000; Deng and Xu 2003; Deng 2004, 2005; Deng et al. 2008, 2009, 2012). The main idea is to have only a small number of nonzero values for the coefficients a_j . They specialize the recurrence (1) to the form

$$x_i = \sum_{a \in \mathcal{A}} a \sum_{j \in S(a)} x_{i-j} \bmod m, \quad (3)$$

where $\mathcal{A} \subset \{1, \dots, m-1\}$ is a small set, usually of cardinality no more than 2 or 3, and $S(a) \subset \{1, \dots, k\}$ for each $a \in \mathcal{A}$. The rationale is to reduce the number of multiplications modulo m required to compute the recurrence.

Their earliest proposal in this family was the FMRG- k generator of Deng and Lin (2000), where $\mathcal{A} = \{m-1, b\}$, $S(m-1) = 1$, and $S(b) = k$, which gives

$$\begin{aligned} x_i &= ((m-1)x_{i-1} + bx_{i-k}) \bmod m \\ &= (-x_{i-1} + bx_{i-k}) \bmod m. \end{aligned} \quad (4)$$

Deng and Xu (2003) and Deng (2005) then proposed a class named DX- k - σ - t (originally with $t = 1$), where $\mathcal{A} = \{b\}$, $S(b) = \{t, k\}$ for $\sigma = 2$, $S(b) = \{t, \lceil k/2 \rceil, k\}$ for $\sigma = 3$, and $S(b) = \{t, \lceil k/3 \rceil, \lceil 2k/3 \rceil, k\}$ for $\sigma = 4$. For $\sigma \geq 2$, this gives

$$x_i = b \sum_{j \in S(b)} x_{i-j} \bmod m. \quad (5)$$

Computing the corresponding recurrence requires a single modular multiplication, by b . For $\sigma = 1$, they take $\mathcal{A} = \{1, b\}$ with $S(1) = \{t\}$ and $S(b) = \{k\}$, which gives $x_i = (x_{i-t} + bx_{i-k}) \bmod m$.

Deng et al. (2008) then proposed the DL- k - t class, where $\mathcal{A} = \{b\}$ and $S(b) = \{t, t+1, \dots, k\}$, which gives

$$\begin{aligned} x_i &= b \sum_{j=t}^k x_{i-j} \bmod m \\ &= x_{i-1} + b(x_{i-t} - x_{i-k-1}) \bmod m, \end{aligned} \quad (6)$$

and the DS- k - t class, where $\mathcal{A} = \{b\}$ and $S(b) = \{1, \dots, t-1, t+1, \dots, k\}$, which gives

$$\begin{aligned} x_i &= b \sum_{j=1, j \neq t}^k x_{i-j} \bmod m \\ &= x_{i-1} + b(x_{i-1} - x_{i-t} + x_{i-t-1} - x_{i-k-1}) \bmod m. \end{aligned} \quad (7)$$

In (6) and (7), the last expression provides an efficient way of implementing the recurrence, with a single multiplication and a small number of additions.

Deng et al. (2012) introduced a modified version of the DX- k - σ - t recurrences, in which $t=1$ and the term x_{i-g} is added to the right side for some integer $g \in \{1, \dots, k\}$. That is, they take $\mathcal{A} = \{1, b\}$, $S(1) = \{g\}$ for $\sigma \geq 2$ and $S(1) = \{1, g\}$ for $\sigma = 1$, and $S(b)$ as for the DX- k - σ - t . They call them DX*- k - σ - g . For example, for $\sigma = 1$, this gives

$$x_i = x_{i-g} + x_{i-1} + bx_{i-k} \bmod m, \quad (8)$$

and for $\sigma = 2$, we have

$$x_i = x_{i-g} + b(x_{i-1} + x_{i-k}) \bmod m. \quad (9)$$

These authors provide specific parameter choices that give a maximal period $m^k - 1$ for k ranging from 101 to 25013, for $m = 2^{31} - c$ for small values of c (Deng and Lin 2000; Deng and Xu 2003; Deng 2004, 2005, 2008; Deng et al. 2012).

Besides a long period, a key requirement for a good random number generator (RNG) is that the set of all vectors of successive output values (u_i, \dots, u_{i+s-1}) , from all possible initial states, should cover the unit hypercube $[0, 1]^s$ very evenly (L'Ecuyer 2006). This requirement captures both uniformity and independence. Indeed, an (ideal) RNG would produce independent uniform random variables over $[0, 1]$ if and only if (u_i, \dots, u_{i+s-1}) has the uniform distribution over the unit hypercube for any i and s . More generally, for any finite set of integers $I = \{i_1, \dots, i_s\}$, where $0 \leq i_1 < \dots < i_s$, consider the multiset $\Psi_s(I)$ of all s -dimensional output vectors $(u_{i_1}, \dots, u_{i_s})$ obtained when the initial state $s_0 = (x_0, \dots, x_{k-1})$ of the MRG runs over all its m^k possibilities:

$$\Psi_s(I) = \{(u_{i_1}, \dots, u_{i_s}) \in [0, 1]^s \mid s_0 \in \mathbb{Z}_m^k\},$$

with $\mathbb{Z}_m = \{0, \dots, m-1\}$. We shall denote by $\tilde{\Psi}_s(I)$ the ordinary set that corresponds to the multiset $\Psi_s(I)$ (it contains a single copy of each point). If s_0 is selected at random uniformly from \mathbb{Z}_m^k , $(u_{i_1}, \dots, u_{i_s})$ has the uniform distribution over $\Psi_s(I)$. For this to be a good approximation of the uniform distribution over $[0, 1]^s$, $\Psi_s(I)$ must cover $[0, 1]^s$ very evenly. Note that if the MRG has maximal period $m^k - 1$ (which we shall assume from now on), then all points of $\Psi_s(I)$ are visited exactly once (or according to their multiplicity

if they appear more than once in the multiset $\Psi_s(I)$) when the MRG runs over its full period, except for the zero vector $(0, \dots, 0)$ which appears one time fewer.

Whenever $i_s - i_1 < k$, $\Psi_s(I)$ contains every vector of $(\mathbb{Z}_m^s)/m$, i.e., every s -dimensional vector whose coordinates are in $\{0, 1/m, \dots, (m-1)/m\}$ exactly m^{k-s} times each. This is the best uniformity we can hope for, given that the output coordinates are all multiples of $1/m$. For $s > k$, this ideal uniformity is of course impossible, because $|\Psi_s(I)| = m^k < m^s$. More interestingly, when $i_s - i_1 \geq k$, this uniformity is no longer guaranteed even if s is small. For this situation, it is known that $\tilde{\Psi}_s(I)$ is the intersection of a lattice in \mathbb{R}^s with the hypercube $[0, 1]^s$ (Knuth 1998, L'Ecuyer 1999a). This implies in particular that there are families of equidistant parallel hyperplanes in \mathbb{R}^s such that each family covers $\Psi_s(I)$. A standard way of measuring the uniformity of $\Psi_s(I)$ then is via the so-called *spectral test* (Knuth 1998): one computes the distance $d_s(I)$ between the hyperplanes of the family for which this distance is largest. We want this distance $d_s(I)$ to be as small as possible, to avoid large empty gaps. It is common practice to standardize this measure into a real number between 0 and 1 defined as $S_s(I) = d_s^*(n)/d_s(I)$, where $d_s^*(n)$ is a lower bound on the smallest possible distance between hyperplanes that can be achieved by a general s -dimensional lattice having n points per unit of volume (Conway and Sloane 1999), and $n = \min(m^k, m^s)$ is the largest possible number of distinct points in $\Psi_s(I)$. Very small values of $S_s(I)$ must be avoided. Good MRGs having reasonably large values of $S_s(I)$ ($S_s(I) > 0.6$, for example) for all I in a large collection of index sets I , including sets with $s = |I| \gg k$, have been constructed (L'Ecuyer 1999a).

A primary purpose of this paper is to study the structure of $\Psi_s(I)$ for the special types of MRGs mentioned earlier, and exhibit index sets I for which $S_s(I)$ is always very small, when $i_s - i_1 \geq k$. This is a sequel to a first analysis made by L'Ecuyer and Touzin (2004) for the RNGs of Deng and Lin (2000) and Deng and Xu (2003).

We also exhibit and explain potential problems that may occur in the initialization of these special types of MRGs. If one is not sufficiently careful about the initialization, the structure of the initial state can easily interact with that of the MRG and be apparent in the output for a large number of steps. We explain why and we show that this may have a disastrous impact on the statistical behavior of the RNG. The reason for this is that the recurrence of those special types of MRGs does not make a sufficiently complicated modification of the state at each step. This type of problem does not occur for MRGs having a smaller state and a more complicated recurrence, such as those proposed

in L'Ecuyer (1999a) and L'Ecuyer and Touzin (2000), for example.

The rest of the article is organized as follows. In §2, we give some background on the lattice structure analysis of MRGs, and provide bounds on a figure of merit that measures the quality of the lattice structure of the set $\Psi_s(I)$ for certain classes of DX, DX*, DL, and DS generators. These bounds show in particular that the lattice structure cannot be good when b , or its inverse modulo m , is small, or when a small multiple of b is close to a small multiple of m , or if b is a sum of two powers of 2 of a certain form. We also manage to bound those bounds uniformly in b ; this yields upper bounds which show that some of these generators cannot have a good lattice structure regardless of the value of b (even for large b). In §3, we compare these bounds with the exact value of the figure of merit for a representative selection of those special types of MRGs. In §4, we illustrate the effect of this lattice structure on the results of a simple empirical statistical test. Section 5 is devoted to problems that can occur with the initialization of these MRGs. It shows that if the initial state has too much structure, then this structure may persist for a very large number of steps. Section 6 offers some conclusions.

2. Lattice Structure

2.1. Vectors of the Dual Lattice

Let $\mathbf{e}_{i(s)}$ denote the i th unit vector in s dimensions, and let $x_{i,0}, x_{i,1}, \dots$, be the sequence obtained from the recurrence (1) when $(x_0, \dots, x_{k-1}) = (x_{i,0}, \dots, x_{i,k-1}) = \mathbf{e}_{i(k)}$, for $i = 1, \dots, k$. It is known (L'Ecuyer and Couture 1997) that $\tilde{\Psi}_s(I) = L_s(I) \cap [0, 1)^s$, where $L_s(I)$ is the lattice generated by the vectors $(x_{i,i_1}/m, \dots, x_{i,i_s}/m)$ for $i = 1, \dots, k$, together with the unit vectors $\mathbf{e}_{1(s)}, \dots, \mathbf{e}_{s(s)}$. From this set of $k + s$ vectors, one can obtain a basis of s linearly independent vectors that generate the same lattice (L'Ecuyer and Couture). The dual lattice $L_s^*(I)$ to $L_s(I)$ is the set of vectors \mathbf{w} such that $\mathbf{w}^t \mathbf{v} \bmod 1 = 0$ for all $\mathbf{v} \in L_s(I)$. If $l_s(I)$ is the Euclidean length of the shortest nonzero vector in $L_s^*(I)$, then $d_s(I) = 1/l_s(I)$. Thus, a small value of $l_s(I)$ means a small value of $S_s(I)$ and poor uniformity of $\Psi_s(I)$. For $s \leq 8$, the smallest possible distance between hyperplanes that can be achieved by a general s -dimensional lattice of density n is known exactly (Conway and Sloane 1999, Knuth 1998); we denote it by $d_s^*(n)$ (the dimension s considered in this paper never exceeds 6).

By putting $a_0 = -1$, we can rewrite (1) as

$$\sum_{j=0}^k a_j x_{i-j} \bmod m = 0. \quad (10)$$

Let $I^* = \{j: 0 \leq j \leq k \text{ and } a_{k-j} \neq 0\}$. For the special case where $0 = i_1 < i_2 < \dots < i_s = k$ and $I^* \subseteq I$, it is

easily seen from (10) (L'Ecuyer 1997) that the vectors $\mathbf{w}_i = m\mathbf{e}_{i(s)}$ for $i = 1, \dots, s-1$ and $\mathbf{w}_s = (a_{k-i_1}, a_{k-i_2}, \dots, a_{k-i_{s-1}}, -1)$ form a basis of $L_s^*(I)$, and that $m\mathbf{e}_{s(s)}$ also belongs to $L_s^*(I)$. The fact that $\mathbf{w}_s \in L_s^*(I)$ implies that

$$l_s^2(I) \leq \|\mathbf{w}_s\|^2 = 1 + a_1^2 + \dots + a_k^2, \quad (11)$$

where $\|\cdot\|$ is the Euclidean norm. Any integer multiple of \mathbf{w}_s modulo m also belongs to $L_s^*(I)$, as well as any linear combination of the form $\mathbf{w} = \sum_{i=1}^s z_i \mathbf{w}_i$ with integer coefficients z_i . Moreover, if $I^* \subseteq I \subset I'$, $s' = |I'| > s$, $\mathbf{w} \in L_s^*(I)$, and \mathbf{w}' is constructed from \mathbf{w} by adding zero coordinates for the $s' - s$ indexes in $I' \setminus I$, then $\mathbf{w}' \in L_{s'}^*(I')$. This implies that $l_{s'}(I') \leq l_s(I)$ and that the bound (11) holds for I' as well.

For any integer w , we denote

$$[w]_m = w - z'm, \quad (12)$$

where z' is the unique integer for which $-m/2 < w - z'm \leq m/2$. This integer minimizes $|w - z'm|$. For a vector $\mathbf{w} = (w_1, \dots, w_s)$ with integer coordinates, we denote $[\mathbf{w}]_m = ([w_1]_m, \dots, [w_s]_m)$. Whenever $\mathbf{w} \in L_s^*(I)$, $[\mathbf{w}]_m \in L_s^*(I)$ as well, because $[\mathbf{w}]_m$ can be obtained from \mathbf{w} by adding an integer linear combination of $m\mathbf{e}_{1(s)}, \dots, m\mathbf{e}_{s(s)}$, which all belong to $L_s^*(I)$. It is also obvious that $\|[\mathbf{w}]_m\| \leq \|\mathbf{w}\|$.

Observe that a vector \mathbf{w} belongs to $L_s^*(I)$ if and only if it can be written as $\mathbf{w} = z\mathbf{w}_s + \sum_{j=1}^s z_j m\mathbf{e}_{j(s)}$ for some integers z, z_1, \dots, z_s . For z fixed, the shortest of those vectors \mathbf{w} is precisely $[z\mathbf{w}_s]_m \in L_s^*(I)$. Thus, the shortest vector in the dual lattice must have the form $[z\mathbf{w}_s]_m$ for some nonzero integer z , which can be taken from $\{1, \dots, m-1\}$ because z can be reduced modulo m . We have just proved the following result:

PROPOSITION 1. *One has*

$$\begin{aligned} l_s^2(I) &= \min_{z \in \{1, \dots, m-1\}} \|[z\mathbf{w}_s]_m\|^2 \\ &= \min_{z \in \{1, \dots, m-1\}} ([za_{k-i_1}]_m^2 + \dots + [za_{k-i_{s-1}}]_m^2 + [z]_m^2). \end{aligned}$$

For the case where $k = 1$, $s = 2$, $I = \{0, 1\}$, and $a_1 = b$, this gives $l_s^2(I) = \min_{z \in \{1, \dots, m-1\}} ([zb]_m^2 + [z]_m^2)$. But it is known (Knuth 1998) that for this special case, for any choices of $m > b > 0$, $l_s^2(I) \leq (4/3)^{1/2}m$. This gives the general inequality:

PROPOSITION 2. *For any integers $m > b > 0$, there is an integer $z \in \{1, \dots, m-1\}$ such that*

$$[zb]_m^2 + [z]_m^2 \leq (4/3)^{1/2}m.$$

In what follows, we will exploit these two propositions to develop refined bounds on $l_s(I)$ for special types of MRGs proposed by Deng and his co-authors. We denote $\tilde{S}(b) = \{k-j \mid j \in S(b), j < k\} \cup \{k\}$.

2.2. Short Dual Lattice Vectors for the DX- k - σ - t Generator

For the DX- k - σ - t with $\sigma \geq 2$, for $I = \{0\} \cup \bar{S}(b)$, we have $\mathbf{w}_s = (b, \dots, b, -1)$, where $s = \sigma + 1$, and therefore $l_s^2(I) \leq \sigma b^2 + 1$. If b^* is the inverse of b modulo m , i.e., $b^*b \bmod m = 1$ (assuming that such a b^* exists; it always does when m is prime, which is typical in our setting), then $\mathbf{w}_s^* \stackrel{\text{def}}{=} b^* \mathbf{w}_s \bmod m = (1, \dots, 1, -b^*)$ also belongs to $L_s^*(I)$, so $l_s^2(I) \leq (b^*)^2 + \sigma$. More generally, for any integer z , $[z\mathbf{w}_s]_m = ([zb]_m, \dots, [zb]_m, [-z]_m) \in L_s^*(I)$, which gives the upper bound

$$l_s^2(I) \leq \sigma [zb]_m^2 + [z]_m^2. \quad (13)$$

If zb is close to a multiple of m for some small integer z , then this bound is particularly small. Likewise, if z^*b^* is close to a multiple of m for a small integer z^* , taking $z = z^*b^*$ in (13) yields $l_s^2(I) \leq \sigma [z^*]_m^2 + [z^*b^*]_m^2$, which is small. In other words, if either b or b^* is near $m/2$, or $m/3$, or $2m/3$, \dots , or zm/i for small integers $z \geq 1$ and $i \geq 2$, then we know a priori that $l_s^2(I)$ must be small, and that the lattice structure of $L_s^*(I)$ cannot be good.

For the DX- k -1- t , a similar argument with $I = \{0, k - t, k\}$ shows that $\mathbf{w}_s = (b, 1, -1) \in L_s^*(I)$, and this gives the upper bound

$$l_s^2(I) \leq [zb]_m^2 + 2[z]_m^2 \quad (14)$$

for all integers z . Taking $z = z^*b^*$, this gives $l_s^2(I) \leq [z^*]_m^2 + 2[z^*b^*]_m^2$. This shows again that if either b or b^* is near zm/i for small integers $z \geq 1$ and $i \geq 2$, then $l_s^2(I)$ must be small and the lattice structure cannot be good.

EXAMPLE 1. One example of DX- k - σ -1 proposed by Deng et al. (2012) has $\sigma = 3$, $m = 2^{31} - 1$, $k = 7499$, and $b = 1073741559$. Here, $2b = 2147483118 = m - 529$ is very close to m . By taking $z = 2$ in (13), the bound evaluates to $(2b - m)^2 \sigma + 2^2 = 839527$. Taking the square root gives $l_s(I) \leq 916.257$, and the corresponding bound on the standardized figure of merit becomes $S_s(I) \leq 3.587 \times 10^{-7}$, which is very small. This bound is actually the exact value in this case.

If we combine Proposition 2 with the bound in (13), we find that for $\sigma \geq 2$, there is a $z > 0$ such that

$$\begin{aligned} l_s^2(I) &\leq \sigma(4/3)^{1/2} m - (\sigma - 1)[z]_m^2 \\ &\leq \sigma(4/3)^{1/2} m - (\sigma - 1), \end{aligned} \quad (15)$$

where the last expression is a bound that does not depend on b . For $\sigma = 1$, a similar argument with (14) gives

$$l_s^2(I) \leq 2(4/3)^{1/2} m - 1. \quad (16)$$

We call L_2^2 the bound in (15) or (16), depending on the value of σ .

We now examine a different way of showing the existence of a small integer z for which zb is close to a multiple of m , i.e., for which $zb/m \bmod 1$ is close to 0 or 1. It will give a slightly different bound. The arithmetic sequence $\{z\alpha \bmod 1, z = 1, 2, 3, \dots\}$, for an arbitrary real number $\alpha > 0$, is well known and has been studied at length in the literature. When α is irrational, it is known as a Weyl sequence. Here we will use a property of this sequence called the *Three Gap Theorem*, first proved by Sós (1958) and revisited by several other authors; see, e.g., van Ravenstein (1988):

THEOREM 1. *Let $\alpha > 0$ be a real number and let $r \geq 1$ be an integer, let $u^{(1)} < \dots < u^{(r)}$ be the values $\{z\alpha \bmod 1, z = 1, \dots, r\}$, sorted by increasing order, and define the gaps $\delta_0 = u^{(1)}$, $\delta_i = u^{(i+1)} - u^{(i)}$ for $i = 1, \dots, r - 1$, and $\delta_r = 1 - u^{(r)}$. Then these $r + 1$ gaps take at most three distinct values, which are δ_0 , δ_r , and (perhaps) $\delta_0 + \delta_r$.*

Clearly, the smallest gap here is $\min(\delta_0, \delta_r) = \min\{|[z\alpha]_1| : 1 \leq z \leq r\}$, and this smallest gap cannot be larger than $1/(r + 1)$, because the sum of the $r + 1$ gaps must add up to 1. Applying this result to our setting for $\alpha = b/m$, we find that there is an integer $z \leq r$ for which $|[zb/m]_1| = |[zb]_m|/m \leq 1/(r + 1)$, and noticing that $[zb]_m$ must be an integer, we obtain:

COROLLARY 1. *For any integer $r \geq 1$, there is an integer $z \in \{1, \dots, r\}$ for which*

$$[zb]_m^2 \leq \lfloor m/(r + 1) \rfloor^2. \quad (17)$$

By plugging this into (13), it follows that for $\sigma \geq 2$, for any $r \geq 1$,

$$l_s^2(I) \leq \sigma \lfloor m/(r + 1) \rfloor^2 + r^2 \stackrel{\text{def}}{=} \varphi(r). \quad (18)$$

Now we can try to minimize this bound with respect to r ; that is, compute

$$L_3^2 \stackrel{\text{def}}{=} \varphi(r^*) = \min_{r \geq 1} \varphi(r).$$

To obtain a crude (initial) estimate of r^* , we will neglect the fact that r must be an integer, ignore the floor function, and replace $r + 1$ by r in (18). This gives the approximate bound $\sigma m^2/r^2 + r^2$. Taking the derivative of this expression with respect to r and equating it to zero, we obtain the equation $-2m^2\sigma r^{-3} + 2r = 0$, for which $r = m^{1/2}\sigma^{1/4}$ is a root, where the expression has a minimum, because the second derivative is positive for $r > 0$. We shall take $x_0 = m^{1/2}\sigma^{1/4}$ as a crude real-valued approximation of r^* , and then search on both sides of x_0 to find the exact integer r^* that minimizes $\varphi(r)$. Another possibility is to just round x_0 to the nearest integer instead of searching for r^* ; in our experiments this made no significant difference. When m is large and σ is small (which is typical), we have $L_3^2 \approx 2m\sigma^{1/2}$.

When comparing L_3^2 with L_2^2 , for $\sigma = 2$, we have $L_2^2 = 2m\sqrt{4/3} - 1 < L_3^2 \approx 2m\sqrt{2}$. For $\sigma = 3$, $L_2^2 = 2m\sqrt{3} - 2 \approx L_3^2 \approx 2m\sqrt{3}$. For $\sigma \geq 4$, $L_2^2 = m\sigma\sqrt{4/3} - (\sigma - 1) > L_3^2 \approx 2m\sqrt{\sigma}$. Either of those bounds can be used to show that $S_s(I)$ cannot be close to 1 regardless of b , for given values of m and k . In the following, we will take the minimum of the two and will denote $L_0 = \min(L_2, L_3)$.

EXAMPLE 2. Consider the DX- k - σ - t generator with $m = 2^{31} - 1 = 2147483647$ and $k = 7499$, also examined in Table 3, in Section 3. For $\sigma = 2$, we have $x_0 = m^{1/2}\sigma^{1/4} \approx 55109$, $r^* = 55115$, and the bound $\varphi(r^*)$ evaluates to $l_s^2(I) \leq \min_{r \geq 1} \varphi(r) = \varphi(r^*) = 6073738113$, or $l_s(I) \leq L_3 = \sqrt{\varphi(r^*)} = 77934.2$ (accurate to the given digits). The corresponding bound on the standardized figure of merit becomes $S_s(I) \leq 3.23316 \times 10^{-5} \ll 1$. We also have $L_2^2 = 2m\sqrt{4/3} - 1$, which gives $L_2 = 70423.0 < L_3$ and $S_s(I) \leq 2.92155 \times 10^{-5}$. These bounds hold for all b . If we take $b = 1038757$, for instance, the exact values are $l_s(I) = 48147.1 \approx 0.684L_2 \approx 0.618L_3$ and $S_s(I) = 1.99741 \times 10^{-5}$.

For $\sigma = 1$, the corresponding numbers are $x_0 = m^{1/2}/2^{1/4} \approx 38968$, $r^* = 38962$, $\varphi(r^*) = 6073738113$, $L_3 = 77934.2$, and this gives $S_s(I) \leq 3.23316 \times 10^{-5} \ll 1$. We also have $L_2 = 70423.0 < L_3$. If we take $b = 967501$, the exact values are $l_s(I) = 52479.3 \approx 0.745L_2 \approx 0.673L_3$ and $S_s(I) = 2.17714 \times 10^{-5}$.

For $\sigma = 4$, we obtain $L_3 = 92679.8 < L_2 = 99593.2$.

2.3. Short Dual Lattice Vectors for the DX*- k - σ - g Generator

For the DX*- k - σ - g with $\sigma \geq 2$, for $I = \{0, g\} \cup \bar{S}(b)$, we obtain $\mathbf{w}_s = (b, \dots, 1, \dots, b, -1)$ with $s = \sigma + 2$, where the position of the 1 depends on the position of g in the ordered set I . We also have that $\mathbf{w}_s^* \stackrel{\text{def}}{=} b^* \mathbf{w}_s \bmod m = (1, \dots, b^*, \dots, 1, -b^*) \in L_s^*(I)$. In this case, the bound given by Proposition 1 becomes $l_s^2(I) \leq \|\mathbf{z}\mathbf{w}_s\|_m^2 = [zb]_m^2 \sigma + 2[z]_m^2$ for all z . For the case where $z = z^*b^*$, this gives $l_s^2(I) \leq \sigma[z^*]_m^2 + 2[z^*b^*]_m^2$. Again, if b or b^* is close to zm/i for some small integers $z \geq 1$ and $i \geq 2$, then $l_s^2(I)$ is necessarily small.

For the DX*- k -1- g , if we take $I = \{0, k - g, k - 1, k\}$, we obtain $\mathbf{w}_s = (b, 1, 1, -1)$ and $\mathbf{w}_s^* = (1, b^*, b^*, -b^*)$, and this leads to $l_s^2(I) \leq [zb]_m^2 + 3[z]_m^2$ and $l_s^2(I) \leq [z^*]_m^2 + 3[z^*b^*]_m^2$ for all integers z and z^* .

2.4. Short Dual Lattice Vectors for the DL- k - t and DS- k - t Generators

For the DL- k - t and DS- k - t , we find from the representations (6) and (7) that they can be seen as MRGs of order $k' = k + 1$. We will use these representations for our lattice structure analysis (the fact that they do not have period $m^{k+1} - 1$ has no impact on this analysis). For the DL- k - t with $t > 1$, for $I = \{0, k - t + 1, k, k + 1\}$, we obtain that both $\mathbf{w} = (-b, b, 1, -1)$ and $\mathbf{w}^* = (-1, 1, b^*, -b^*)$ are in $L_s^*(I)$. This leads to

$l_s^2(I) \leq 2[zb]_m^2 + 2[z]_m^2$ and $l_s^2(I) \leq 2[z^*b^*]_m^2 + 2[z^*]_m^2$ for all z and z^* .

For the DL- k -1, for $I = \{0, k, k + 1\}$, we obtain that both $\mathbf{w} = (-b, b + 1, -1)$ and $\mathbf{w}^* = (-1, 1 + b^*, -b^*)$ are in $L_s^*(I)$. This gives $l_s^2(I) \leq [zb]_m^2 + [z(b + 1)]_m^2 + [z]_m^2$ and $l_s^2(I) \leq [z^*b^*]_m^2 + [z^*(b^* + 1)]_m^2 + [z^*]_m^2$ for all z and z^* .

Likewise, for the DS- k - t , for $I = \{0, k - t, k - t + 1, k, k + 1\}$, we find that both $\mathbf{w} = (-b, b, -b, b + 1, -1)$ and $\mathbf{w}^* = (-1, 1, -1, b^* + 1, -b^*)$ are in $L_s^*(I)$, and from this we obtain $l_s^2(I) \leq 3[zb]_m^2 + [z(b + 1)]_m^2 + [z]_m^2$ and $l_s^2(I) \leq [z^*b^*]_m^2 + [z^*(b^* + 1)]_m^2 + 3[z^*]_m^2$ for all z and z^* .

2.5. Summary of Upper Bounds on $l_s^2(I)$

Table 1 summarizes the bounds on $l_s^2(I)$ derived so far in this section. Each bound depends on the choice of a small integer $z \geq 1$ or $z = z^*b^*$ (in which case $zb = z^*$) for a small $z^* \geq 1$. In the remainder of the paper, we use $L_1^2(z)$ to denote the upper bound on $l_s^2(I)$ given in the table, for each considered type of MRG. The bounds $L_1^2(z)$ in this table are small (and typically tight) for some small z or z^* when a small multiple of either b or b^* is close to a small multiple of m . As a special case, the bounds are small when b or b^* is small.

In general, we can apply Proposition 2 and Corollary 1 to these bounds, as we did in (15) and (18), to obtain a set of bounds L_2^2 and L_3^2 that hold uniformly in b . Corollary 1 gives a bound that depends on r , of the general form $l_s^2(I) \leq \varphi(r)$ for all $r \geq 1$, where the function φ depends on the type of generator and is given in Table 2. The table also gives a crude real-valued estimate x_0 of $r^* = \arg \min_{r \geq 1} \varphi(r)$. The corresponding bound $\varphi(r^*)$ on $l_s^2(I)$ is named L_3^2 . Note that for the DL and DS generators, we use the fact that $[z(b + 1)]_m^2 \leq [zb]_m^2 + 2[zb]_m|z| + [z]_m^2 \leq [m/(r + 1)]^2 + 2[m/(r + 1)]r + r^2$ to obtain our φ .

In §3, we compute and compare these bounds with the exact values of $l_s(I)$ and $S_s(I)$, for several specific MRGs proposed by Deng and his co-authors. In our examples, the bound $L_0 = \min(L_2, L_3)$ will never be reached exactly, but will often be within a factor of 2 or 3 from the exact value.

Table 1 Bounds $L_1^2(z)$ and L_2^2 on $l_s^2(I)$ for Special Types of MRGs

	$L_1^2(z)$	L_2^2
DX- k - σ - t for $\sigma \geq 2$	$\sigma[zb]_m^2 + [z]_m^2$	$\sigma(4/3)^{1/2}m - (\sigma - 1)$
DX- k -1- t	$[zb]_m^2 + 2[z]_m^2$	$2(4/3)^{1/2}m - 1$
DX*- k - σ - g for $\sigma \geq 2$	$\sigma[zb]_m^2 + 2[z]_m^2$	$\sigma(4/3)^{1/2}m - (\sigma - 2)$
DX*- k -1- g	$[zb]_m^2 + 3[z]_m^2$	$3(4/3)^{1/2}m - 2$
DL- k - t with $t > 1$	$2[zb]_m^2 + 2[z]_m^2$	$2(4/3)^{1/2}m$
DL- k -1	$[zb]_m^2 + [z(b + 1)]_m^2 + [z]_m^2$	$2(4/3)^{1/2}m - 1$
DS- k - t	$3[zb]_m^2 + [z(b + 1)]_m^2 + [z]_m^2$	$4(4/3)^{1/2}m - 3$

Table 2 Expressions for x_0 and $\varphi(r)$ for the Bounds L_3^2 , for Special Types of MRGs

	x_0	$\varphi(r)$
DX- k - σ - t for $\sigma \geq 2$	$m^{1/2}\sigma^{1/4}$	$\lfloor m/(r+1) \rfloor^2 \sigma + r^2$
DX- k -1- t	$m^{1/2}2^{-1/4}$	$\lfloor m/(r+1) \rfloor^2 + 2r^2$
DX*- k - σ - g for $\sigma \geq 2$	$m^{1/2}(\sigma/2)^{1/4}$	$\lfloor m/(r+1) \rfloor^2 \sigma + 2r^2$
DX*- k -1- g	$m^{1/2}3^{-1/4}$	$\lfloor m/(r+1) \rfloor^2 + 3r^2$
DL- k - t with $t > 1$	$m^{1/2}$	$2(\lfloor m/(r+1) \rfloor^2 + r^2)$
DL- k -1	$m^{1/2}$	$2(\lfloor m/(r+1) \rfloor^2 + \lfloor m/(r+1) \rfloor r + r^2)$
DS- k - t	$m^{1/2}2^{1/4}$	$2(2\lfloor m/(r+1) \rfloor^2 + \lfloor m/(r+1) \rfloor r + r^2)$

2.6. Bounds on $l_s^2(I)$ When $b = 2^w + 2^r$ and $m = 2^{31} - 1$

Deng et al. (2012) propose several generators with coefficients of the special form $b = 2^r \pm 2^w$, where $31 > r > w > 0$, for $m = 2^{31} - 1$. In our experiments, we found that for those types of generators, in most cases $L_1(z)$ was minimized and equal to $l_s(I)$ for z equal to a power of 2 (see Tables 4–7). To explain this, observe that by taking $z = 2^e$ for some integer $e > 0$, we have in this case

$$[zb]_m^2 = [2^e(2^r \pm 2^w)]_m^2 = [2^{e+r} \pm 2^{e+w}]_m^2, \quad \text{and}$$

$$[z(b+1)]_m^2 = [2^e(2^r \pm 2^w + 1)]_m^2 = [2^{e+r} \pm 2^{e+w} + 2^e]_m^2.$$

Knowing that $[2^{31}]_m = 1$ and $w < r$, it is easily seen that $[zb]_m^2$ is minimized by taking $e = 31 - w$ if $r - w \leq 15$ and $e = 31 - r$ when $r - w \geq 16$. However, the bound $L_1(z)$ itself can be minimized by another value of e , because it contains other terms, namely $[z]_m^2$ and in some cases $[z(b+1)]_m^2$. With $e = 31 - w$, we have

$$[zb]_m^2 = [2^{r-w} \pm 1]_m^2, \quad \text{and}$$

$$[z(b+1)]_m^2 = [2^{r-w} \pm 1 + 2^{31-w}]_m^2,$$

which are small when w is not too far from 31 (in which case both $31 - w$ and $r - w$ must be small), whereas taking $e = 31 - r$ gives

$$[zb]_m^2 = [1 \pm 2^{31-(r-w)}]_m^2, \quad \text{and}$$

$$[z(b+1)]_m^2 = [1 \pm 2^{31-(r-w)} + 2^{31-r}]_m^2,$$

which are small when both r and $r - w$ are not too far from 31 (that is, r is large and w is small). By plugging these values of $[zb]_m^2$ and $[z(b+1)]_m^2$ in the bounds $L_1^2(z)$ of Table 1, for any $e > 0$, we obtain special instances of the bounds which are often equal to the exact values, according to our numerical experiments in §3.

EXAMPLE 3. Consider the DX- k -2-64 generator with $m = 2^{31} - 1$, $k = 7499$ and $b = 2^{29} + 2^{17}$, taken from Table 2 of Deng et al. (2012). Here, $w = 17$, so $31 - w = 14$. We compute $L_1^2(2^{14}) = 302006274$, which gives $l_s(I) \leq L_1(2^{14}) = 17378.3$, and then $S_s(I) \leq 7.210 \times 10^{-6}$, which is very small. This bound is actually the exact value in this case.

3. Bounds and Exact Spectral Test Figures for Some Proposed Generators

Here we consider a representative selection of parameters proposed by Deng et al. (2012) for DX, DX*, DL, and DS generators; we compute the exact spectral test values $l_s(I)$ and $S_s(I)$ defined in §2; and compare these values with the bounds $L_1(z)$ in Table 1, computed for a few small values of z , and the bound $L_0 = \min(L_2, L_3)$ defined earlier. We computed the bound $L_1(z)$ for $z = 1, \dots, 25$ and $z = b^*, \dots, 25b^*$, and also for $z = 2^e$ for $e = 0, \dots, 30$, in the situations where $b = 2^w \pm 2^r$. The number 25 was selected arbitrarily. We report in the tables the maximum of $l_s(I)/L_1(z)$ over these values of z , the value of z where the maximum was reached (with a single exception, it was always reached for $z = 1$ or z equal to a power of 2), and the value of $l_s(I)/L_0$. We actually made these computations for all the generators proposed in the above-named papers and the results reported here are representative of what we have observed.

Table 3 gives the values for some DX- k - σ -1 generators taken from Table 1 of Deng et al. (2012). The row with $(\sigma, b) = (3, 1073735056)$ corresponds to Example 1, and those with other values of σ correspond to Example 2. A key observation is that the normalized spectral test value $S_s(I)$ is much smaller than 1 in all cases, and it is not significantly larger on average for larger values of b . Looking at the ratio $l_s(I)/L_0$, we also find that there is no hope to find a value of b for which $S_s(I)$ will be significantly larger (as we saw in Example 2). This means the lattice structure of the set $\Psi_s(I')$ is always bad, for any I' that contains the set I considered here.

Looking at the bounds more closely, we find as expected that when $b < m^{1/2}$, then $L_1(1) < L_0$, and the bound $L_1(1)$ is also equal to the exact value in this case. For larger b , we find four situations where b is close to $m/2 = 1073741823.5$. In fact, $m - 2b$ takes

Table 3 Spectral Test Values and Bounds for the DX- k - σ -1 with $m = 2^{31} - 1$ and $k = 7499$

σ	b	$l_s(I)$	$S_s(I)$	z	$l_s(I)/L_1(z)$	$l_s(I)/L_0$
1	13620	13620.0	5.650e-6	1	1	0.1934
1	967501	52479.3	2.177e-5	25b*	0.7961	0.7452
1	1073735056	13535.0	5.615e-6	2	1	0.1922
2	18178	25707.6	1.066e-5	1	1	0.3650
2	1038757	48147.1	1.997e-5	1	0.0328	0.6837
2	1073706686	46773.4	1.940e-5	2	0.4706	0.6642
3	2307	3995.8	1.564e-6	1	1	0.0463
3	517486	39856.1	1.561e-5	1	0.0445	0.4621
3	1073741559	916.3	3.588e-7	2	1	0.0106
4	25972	51944.0	1.965e-5	1	1	0.5605
4	519708	54539.0	2.063e-5	1	0.0525	0.5885
4	1073723713	63674.5	2.408e-5	2	0.8790	0.6870

Table 4 Spectral Test Values and Bounds for the DX- k - σ - t with $m = 2^{31} - 1$ and $k = 7499$

σ	t	b	$l_s(I)$	$S_s(I)$	z	$l_s(I)/L_1(z)$	$l_s(I)/L_0$
1	29	$1048832 = 2^{20} + 2^8$	5796.8	2.405e-6	2^{11}	0.0111	0.0823
2	64	$537001984 = 2^{29} + 2^{17}$	17378.3	7.210e-6	2^{14}	1	0.2468
3	70	$134479872 = 2^{27} + 2^{18}$	8240.0	3.227e-6	2^{13}	1	0.0955
4	11	$1048578 = 2^{20} + 2^1$	8446.1	3.195e-6	2^{11}	1	0.0911

Table 5 Spectral Test Values and Bounds for the DX*- k - σ - g with $m = 2^{31} - 1$ and $k = 7499$

σ	g	b	$l_s(I)$	$S_s(I)$	z	$l_s(I)/L_1(z)$	$l_s(I)/L_0$
1	45	$134217984 = 2^{27} + 2^8$	4097.1	1.604e-6	16	1	0.0475
1	193	$8388612 = 2^{23} + 2^2$	1116.8	4.373e-7	2^8	1	0.0129
1	360	$528384 = 2^{19} + 2^{12}$	28454.9	1.114e-5	1	0.0539	0.3299
1	383	$1074003968 = 2^{30} + 2^{18}$	14768.6	5.783e-6	2^{13}	1	0.1712
2	17	$134217792 = 2^{27} + 2^6$	1449.7	5.677e-7	16	1	0.0206
2	222	$536870944 = 2^{29} + 2^5$	182.5	7.147e-8	4	1	0.0026
2	257	$536871040 = 2^{29} + 2^7$	725.5	2.841e-7	4	1	0.0103
3	197	$541065216 = 2^{29} + 2^{22}$	757.8	2.866e-7	2^9	1	0.0088
3	257	$4198400 = 2^{22} + 2^{12}$	7237.1	2.737e-6	2^{19}	0.0098	0.0839
3	496	$268500992 = 2^{28} + 2^{16}$	46881.1	1.773e-5	2^{15}	1	0.5435
4	69	$67633152 = 2^{26} + 2^{19}$	5798.4	2.092e-6	2^{12}	1	0.0582
4	131	$536871040 = 2^{29} + 2^7$	1026.0	3.702e-7	4	1	0.0103
4	345	$1074790400 = 2^{30} + 2^{20}$	3548.4	1.280e-6	2^{11}	1	0.0356

the values 13535, 70275, 529, 36221 for $\sigma = 1, 2, 3, 4$, respectively, in those situations. For the two smallest values of $m - 2b$, for $\sigma = 1$ and 3, the bound $L_1(2)$ is equal to the exact value of $l_s(I)$ (we saw this in Example 1 for $\sigma = 3$). For the two other cases, for $\sigma = 2$ and 4, the bound is close to the exact $l_s(I)$, and closer when $m - 2b$ is smaller. There is also one lucky situation where $z = 25b^*$ gave a pretty tight bound, $L_1(z)$. For the three cases with a medium value of b and $\sigma \geq 2$, the bound L_0 is much tighter than $L_1(z)$ for the values of z that we have examined, and roughly within a factor of two of the exact value. The bound L_0 is very loose in cases where $l_s(I)$ is unusually small; this is not surprising because this bound is the same for all b .

Table 4 gives the results for a few representative DX- k - σ - t generators with $t > 1$, taken from Table 2 of Deng et al. (2012). They all have b of the form $b = 2^r + 2^w$. Again, $S_s(I)$ is very small (bad) in all cases. Here we see that the bound $L_1(z)$ is exact for $z = 2^{31-w}$, when w is large (17 and 18) and for $z = 2^{31-r}$ when w is much smaller than r (the case where $w = 1$). The case with $\sigma = 2$ is Example 3. For $z \leq 25$ or $z^* \leq 25$, the bound $L_1(z)$ (not shown) turns out to be very loose in all cases here. In most cases, it is smaller than L_0 , which is already not very tight.

Table 5 reports some results with DX*- k - σ - g generators taken from Table 3 of Deng et al. (2012), all with $b = 2^r + 2^w$. Again, $S_s(I)$ is very small in all cases, and the ratio $l_s(I)/L_0$ shows that it cannot get much larger. Here we find situations where zb is close

to m for $z = 4$ and for $z = 16$. Note that for $b = 134217984$ and 134217792 , we have $m - 16b = -4097$ and -1025 , respectively, while for $b = 536870944$ and 536871040 , we have $m - 4b = -129$ and -513 , respectively. In those situations, $L_1(z) = l_s(I)$ for $z = 4$ or 16 , and $S_s(I)$ is very small. This is also true for $z = 2^{31-w}$ in all cases where $w \geq 16$ and for $z = 2^{31-r}$ in all cases where $r - w \geq 16$. Note that for the cases mentioned above where the bound is exact for $z = 4$ or $z = 16$, this z also happens to equal 2^{31-r} and w is small in all those cases, so this choice of z is justified in two different ways.

Tables 6 and 7 report some results for DL and DS generators taken from Tables 1 and 2 of Deng et al. (2012), with $s = k + 1$. Again, $S_s(I)$ is very small in all cases. In the two situations where b is small, $L_1(1)$ is the exact value, while when $2b$ is close to m , namely $m - 2b = 21637$ for $b = 1073731005$, and $m - 2b = 49805$ for $b = 1073716921$, $L_1(2)$ is close or equal to the exact value. Another case where $L_1(z)$ is the exact value has $b = 2^{21} + 2^2$, with $r - w = 19$ and $z = 2^{10}$.

Table 6 Spectral Test Values and Bounds for the DL- k - t with $m = 2^{31} - 1$, $k = 7499$

t	b	$l_s(I)$	$S_s(I)$	z	$l_s(I)/L_1(z)$	$l_s(I)/L_0$
1	38999	55153.6	2.288e-5	1	1	0.7832
1	1035347	15569.0	6.459e-6	1	0.0106	0.2211
1	1073716921	53868.4	2.235e-5	2	0.7648	0.7649
13	$2097280 = 2^{21} + 2^7$	23169.6	9.073e-6	2^{10}	0.1250	0.3290
125	$2097156 = 2^{21} + 2^2$	5972.3	2.339e-6	2^{10}	1	0.0848

Table 7 Spectral Test Values and Bounds for the DS- k - t with $m = 2^{31} - 1$, $k = 7499$

t	b	$I_s(I)$	$S_s(I)$	z	$I_s(I)/L_1(z)$	$I_s(I)/L_0$
3,750	26908	53816.5	2.036e-5	1	1	0.5404
3,750	451111	45360.0	1.716e-5	1	0.0503	0.4555
3,750	1073731005	43273.0	1.637e-5	2	1	0.4345
3,754	$1048832 = 2^{20} + 2^8$	5631.7	2.130e-6	2^{11}	0.0054	0.0565
3,915	$1050624 = 2^{20} + 2^{11}$	15596.2	5.899e-6	2^{20}	0.0105	0.1566

4. Some Empirical Statistical Tests

We now show the potential impact of the small spectral test value $S_s(I)$ on the empirical behavior of these generators, via a standard statistical test called the birthday spacings test (Marsaglia 1985, Knuth 1998), in the form studied by L'Ecuyer and Simard (2001) and implemented in TestU01 (L'Ecuyer and Simard 2007). For this test, we select two positive integers n and d , and we generate n points $\mathbf{u}_0, \dots, \mathbf{u}_{n-1}$ "independently" in the d -dimensional unit hypercube $[0, 1]^d$, by calling the RNG d times (once for each coordinate) for each point. We partition $[0, 1]^d$ into $c = 2^{rd}$ cubic boxes of equal size by dividing the interval $[0, 1]$ into 2^r equal parts for some integer r . These boxes are numbered from 0 to $c - 1$, in lexicographic order of the coordinates. Let $K_{(1)} \leq K_{(2)} \leq \dots \leq K_{(n)}$ be the box numbers, sorted by increasing order, where the n points fall and define the spacings $S_j = K_{(j+1)} - K_{(j)}$, for $j = 1, \dots, n - 1$. The test statistic is the number Y of collisions between the spacings, defined as the number of values of $j \in \{1, \dots, n - 2\}$ such that $S_{(j+1)} = S_{(j)}$, where $S_{(1)}, \dots, S_{(n-1)}$ are the spacings sorted by increasing order. Under the null hypothesis, \mathcal{H}_0 , that the generator's output is perfectly random, Y is approximately a Poisson random variable with mean $\lambda = n^3/4c$ if c is large while λ is not too large (L'Ecuyer and Simard 2001). If y denotes the observed value of Y , then the right p -value of the test is $p^+ \stackrel{\text{def}}{=} P[Y \geq y \mid Y \sim \text{Poisson}(\lambda)]$.

Table 8 gives the right p -values of the birthday spacings test for selected generators with $m = 2^{31} - 1$ and $k = 7499$, examined earlier. They were initialized with the combined Tausworthe generator LFSR113 from L'Ecuyer (1999b) (see §5). The points are constructed as $\mathbf{u}_i = (u_{ij_d+j_1}, \dots, u_{(i+1)j_d})$, for $i = 0, \dots, n - 1$, with $I = \{j_1, \dots, j_d\}$ as given in the table. The p -values

Table 8 Right p -Values for the Birthday Spacings Tests with n Points in d Dimensions and c Boxes

RNG	b	I	d	n	c	p^+
DX- k -1-29	1048832	(0, 7470, 7499)	3	2^{19}	2^{54}	5.8×10^{-64}
DX- k -2-64	537001984	(0, 7435, 7499)	3	2^{20}	2^{54}	1.2×10^{-97}
DX- k -3-70	134479872	(0, 3749, 7429, 7499)	4	2^{23}	2^{64}	1.5×10^{-19}
DL- k -125	2097156	(0, 7375, 7499, 7500)	4	2^{23}	2^{64}	1.5×10^{-19}
DX*- k -2-257	536871040	(0, 7242, 7498, 7499)	4	2^{20}	2^{56}	8.3×10^{-37}

indicate spectacular failures of the tests. The explanation is that for the given choice of I , the points have a poor lattice structure, as we saw earlier, and the test detects this structure. For sets I composed of successive output values instead of the I in the table, the test results depend on the initialization, as we will see in the next section.

5. Initialization Problems

5.1. Initializing an MRG with an LCG

MRGs with a large k have a large state, which must be initialized before use. When k exceeds a few dozen, it is common practice to initialize the state using another RNG, whose state is much smaller and easier to initialize. For example, a simple linear congruential generator (LCG) is often used. Taking the same modulus m for the LCG and for the MRG simplifies things even further, because then, k successive integers x_i produced by the LCG can be used directly for the initial state of the MRG. But this type of initialization leads to serious problems, as noted by Matsumoto et al. (2007): the successive values x_i in the initial state have an affine dependence dictated by the LCG and this dependence (or structure) tends to remain for a large number of steps after the initialization. An MRG initialized in this way may fail many simple statistical tests, just like the LCG that was used for initialization. To avoid this type of problem, Matsumoto et al. recommend that MRGs with a large k be initialized using either a generator with a modulus m different from the modulus of the MRG, or with a generator of a different type than an MRG.

For a concrete illustration of this problem, consider the DX- k -1-382 generator with $m = 2^{31} - 1$, $k = 20897$, and $b = 134217736$, from Deng et al. (2012). We initialize this MRG using the LCG based on the recurrence $y_{i+1} = 16807y_i \bmod 2^{31} - 1$. We submit the MRG to the following three empirical tests described in the user's guide of TestU01 (L'Ecuyer and Simard 2007), after reinitializing the generator each time with the given LCG: the *birthday-spacing* test with sample size $n = 2^{14}$ and $c = 2^{40}$ cells in $d = 2$ dimensions, the *collision* test with sample size $n = 2^{17}$ and $c = 2^{36}$ cells in $d = 2$ dimensions, and the *maximum-of- t* test with sample size $n = 2^{18}$, taking the maximum of each group of five successive values and using 2^{14} categories for the chi-square test. The DX- k -1-382 had spectacular failures in all three tests, with a p -value smaller than 10^{-300} in each case, regardless of the choice of initial state of the LCG. When we initialize the same generator with the LFSR113 from L'Ecuyer (1999b), it passes all three tests.

As another example, we applied a birthday spacings test with $n = 2^{22}$ and $c = 2^{60}$ cells in $d = 2$ dimensions to a set of DX- k - σ - t generators with $k = 20897$,

$m = 2^{31} - 1$, and $t \geq 23$, taken from Table 2 of Deng et al. (2012), also initialized with the LCG based on $y_{i+1} = 16807y_i \bmod 2^{31} - 1$. We observed spectacular failures, with several p -values smaller than 10^{-300} . In all cases, the number of collisions was much larger than expected. Because of the large first lag t in these generators, any update of an x_i will have no influence on the next updated x_{i+j} for $j < t$. As a consequence, if there is a simple dependence between the x_i at any time, blocks of t (or less) successive x_i will carry a similar dependence for many steps, and this can explain our empirical results. When the first lag is set to $t = 1$ in these generators, they pass the test.

5.2. Simple Initialization for the DX, DX*, DL Generators

Another easy way to initialize an MRG when k is large is to set all x_i in the initial state to the same nonzero integer value, say $x_{i-k} = c$ for $i = 1, \dots, k$, or perhaps to use $x_{i-k} = i - 1$ for $i = 1, \dots, k$. These types of states appear in the period of the MRG, so taking one of them as the initial state should not be a problem for robust MRGs. In fact, the default initial state in the widely used RNG software of L'Ecuyer et al. (2002) has this form, with all initial values set to $c = 12345$, and this causes no problem. We now show that for the class of generators examined in this paper, these types of initializations are very bad.

For a concrete illustration, we take a DX- k -1- t generator with $m = 2^{31} - 1$, $k = 20897$, $b = 134217736$, and $t = 382$, from Deng et al. (2012). We initialize it with $x_{i-k} = 12345$ for $i = 1, \dots, k$, then we generate and plot the (overlapping) output pairs (u_i, u_{i+1}) , for $i = 1, \dots, 1000$; see the left panel of Figure 1. Interestingly, two of the three points lying on the main diagonal are repeated exactly $t - 1 = 381$ times, and the third one is repeated 236 times. The other two points appear only once. In the right panel, we see

the points $(u_{\nu+i}, u_{\nu+i+1})$, for $i = 1, \dots, 1000$, for $\nu = 10^6$, i.e., after discarding the first one million values. There are still 874 points lying exactly on the diagonal, and some of them are repeated several times: 59 are repeated 10 times, 56 are repeated four times, and 12 are repeated five times.

To understand what happens here, recall that the recurrence for the DX- k -1- t generator is $x_i = (x_{i-t} + bx_{i-k}) \bmod m$. If we initialize x_{-k+1}, \dots, x_0 to the same constant $c > 0$ and use this recurrence to compute x_1, x_2, \dots , we find that x_1, \dots, x_t are all equal to $(b+1)c \bmod m$; then x_{t+1}, \dots, x_{2t} are all equal to $(2b+1)c \bmod m$; then x_{2t+1}, \dots, x_{3t} are all equal to $(3b+1)c \bmod m$; and so on, up to x_k . Starting from x_{k+1} , we still observe blocks of equal successive values, but these blocks have lengths smaller than t . When k is very large and t is large, as in our example, it takes a very long time before these blocks of equal successive values disappear completely. This property holds regardless of the value of c .

If we do the same initialization ($x_{-k+1} = \dots = x_0 = c > 0$) for the DX- k - σ - t in (5) with $\sigma \in \{2, 3, 4\}$, we find a similar behavior. We have $x_i = \sigma bc \bmod m$ for $i = 1, \dots, t$, then $x_i = (\sigma b + \sigma - 1)bc \bmod m$ for $i = t + 1, \dots, 2t$, then $x_i = [b(\sigma b + \sigma - 1) + \sigma - 1]bc \bmod m$ for $i = 2t + 1, \dots, 3t$, then $x_i = [b(b(\sigma b + \sigma - 1) + \sigma - 1) + \sigma - 1]bc \bmod m$ for $i = 3t + 1, \dots, 4t$, and so on, as long as $i \leq [k/(\sigma - 1)]$. For larger indexes i , successive x_i will be equal by smaller groups, depending on the values of k , t , and σ , and the average group sizes will generally decrease with i . Plots for the DX- k -4- t generator with $m = 2^{31} - 1$, $k = 20897$, $b = 268435968$, and $t = 148$, taken from Deng et al. (2012), give a similar pattern as in Figure 1.

These generators have a very poor *diffusion capacity*, in the sense that a strong dependence between values in the initial state needs a very large number of steps before it disappears.

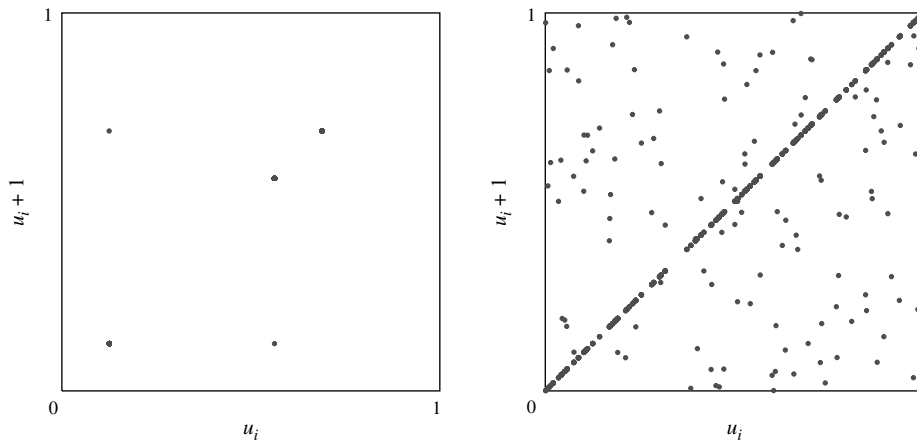


Figure 1 The 1000 Pairs $(u_{\nu+i}, u_{\nu+i+1})$ Produced by the DX- k -1- t Generator with $m = 2^{31} - 1$, $k = 20897$, $b = 134217736$, and $t = 382$, with Initial State $x_{-k+1} = \dots = x_0 = 12345$, for $\nu = 0$ (Left panel) and $\nu = 10^6$ (Right panel)

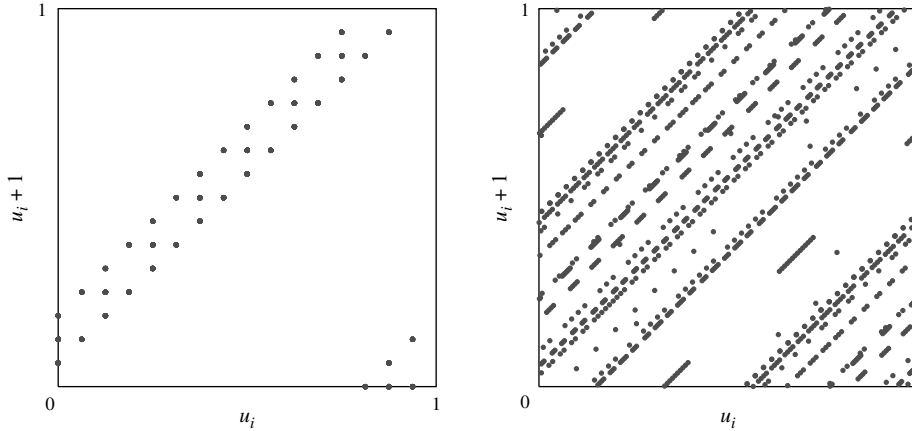


Figure 2 The 1000 Pairs $(u_{\nu+i}, u_{\nu+i+1})$ Produced by the DX- k -1- t Generator with $m = 2^{31} - 1$, $k = 20897$, $b = 134217736$, and $t = 382$, with Initial State Given by $x_{i-k} = i - 1$ for $i = 1, 2, \dots, k$, for $\nu = 0$ (Left panel) and $\nu = 10^5$ (Right panel)

We now initialize the DX- k -1- t generator mentioned earlier with $x_{i-k} = i - 1$ for $i = 1, 2, \dots, k$, and repeat the same experiment as above, except that we now discard the first 10^5 generated values for the right panel. The plots are in Figure 2. Again, these points are far from looking like uniform random points. On the left panel, several points are repeated and lie on just a few lines of slope 1. On the right panel, they still lie on a limited number of lines of slope 1.

To explain this behavior, note that for the recurrence $x_i = (x_{i-t} + bx_{i-k}) \bmod m$, where x_{-k+1}, \dots, x_0 are initialized to $x_{i-k} = i - 1$ for $i = 1, 2, \dots, k$, we have that $x_i = ((b+1)i - t + k) \bmod m$ for $i = 1, \dots, t$, then $x_i = ((2b+1)i - (b+2)t + k) \bmod m$ for $i = t+1, \dots, 2t$, then $x_i = ((3b+1)i - 3(b+1)t + k) \bmod m$ for $i = 2t+1, \dots, 3t$, etc. This implies that groups of $t-1$ pairs (u_i, u_{i+1}) will lie on the same line with slope 1, with each of those lines intersecting the vertical and horizontal axes at different points. The first line (that contains the first $t-1$ pairs) intersects the vertical axis at $(b+1)/m$; the second line (that contains the pairs (u_i, u_{i+1}) for $i = t+1, \dots, 2t-1$) intersects the vertical axis at $(2b+1)/m$; and so on. The slope of the line that connects two successive points is equal to $(u_{i+1} - u_i)/(u_i - u_{i-1})$.

We made similar plots with the DX- k -4- t generator with $m = 2^{31} - 1$, $k = 20897$, $b = 268435968$, and $t = 148$, taken from Deng et al. (2012), and observed similar behavior as in Figure 2.

For the DX*- k -1- g generator (8) initialized with x_{-k+1}, \dots, x_0 all equal to $c > 0$, one easily finds that $x_i = c(ib + i + 1) \bmod m$ for $i = 1, \dots, g$, and therefore, $(x_{i+1} - x_i) = (b+1)c \bmod m$ for $i = 1, \dots, g-1$. That is, the first $g-1$ points (u_i, u_{i+1}) are all (modulo 1) on a line of slope 1 that intersects the vertical axis at $(b+1)c/m \bmod 1$. Although the structure of the following points is a bit more complicated, the second difference $(x_{i+2} - 2x_{i+1} + x_i) \bmod m$ between the successive values is the same for all $i = g+1, \dots, 2g-2$;

then the third difference is the same for $i = 2g+1, \dots, 3g-3$; and so on. The equality of the second differences would show up more clearly in three-dimensional plots of the triples (u_i, u_{i+1}, u_{i+2}) ; that of the third differences would show up in four-dimensional plots; and so on.

The left panel of Figure 3 plots the first 1,000 points generated by the DX*- k -1- g generator with $m = 2^{31} - 1$, $k = 20897$, $b = 537001984$, and $g = 499$, taken from Deng et al. (2012), initialized with $x_i = c = 12345$ for $i = -k+1, \dots, 0$. The visible diagonal line contains the first 498 points and intersects the vertical axis at $(b+1)c/m \bmod 1 = 0.0034$. In the right panel, we initialized the generator with $x_{i-k} = i - 1$ for $i = 1, 2, \dots, k$. The generated points also exhibit a lot of structure.

For the DL- k - t generator (6) defined by the recurrence $x_i = b(x_{i-t} + \dots + x_{i-k}) \bmod m$, initialized with x_{-k+1}, \dots, x_0 all equal to $c > 0$, we find that $x_i = bc(k-t+1) \bmod m$ for $i = 1, \dots, t$, so the points (u_i, u_{i+1}) are all on the main diagonal for $i = 1, \dots, t-1$. Then, $x_{t+i} = bc(k-t+i-1 + i(k-t+1))$ for $i = 1, \dots, t$, which implies that $(u_{i+1} - u_i) \bmod 1 = bc(k-t)/m$ for $i = t+1, \dots, 2t-1$, and therefore the points (u_i, u_{i+1}) are all on a line of slope 1 (modulo 1). Then, the second difference $(u_{i+2} - 2u_{i+1} + u_i) \bmod 1$ is the same for all $i = 2t+1, \dots, 3t-2$, and so on. This generator also exhibits a poor diffusion capacity.

It is interesting to observe that if we use the equivalent recurrence $x_i = x_{i-1} + b(x_{i-t} - x_{i-k-1}) \bmod m$ to implement this generator, as recommended by Deng et al. (2008), and initialize it with $x_{i-k} = c$ for $i = -k, \dots, 0$, then we obtain $x_i = c$ for all $i \geq 1$ as well. That is, the generator always outputs the same value. To avoid this type of problem, it is important to start this recurrence from an initial state that obeys the original recurrence, that is, for which $x_0 = b(x_{-t} + \dots + x_{-k}) \bmod m$. Otherwise, the modified recurrence

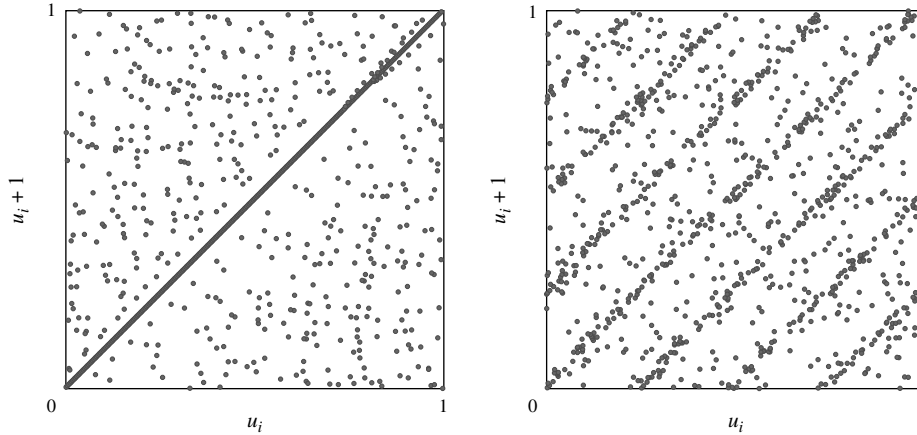


Figure 3 The 1000 Pairs (u_i, u_{i+1}) Produced by the $DX^*-k-1-g$ Generator with $m = 2^{31} - 1$, $k = 20897$, $b = 537001984$, and $g = 499$, with Initial State $x_{-k+1} = \dots = x_0 = 12345$ (Left panel), and $x_{i-k} = i - 1$ for $i = 1, 2, \dots, k$ (Right panel)

may end up in a cycle of length much smaller than $m^k - 1$.

5.3. Initialization Problems for Other Similar Generators

Several other widely available generators have the same lack of diffusion capacity that we just illustrated and are plagued by the same initialization problems. They include, for example, the additive lagged Fibonacci, the add-with-carry (AWC) and subtract-with-borrow (SWB), and the generalized feedback shift register (GFSR) generators. These generators may have a huge period, but if they happen to hit a region where the state has a lot of structure between the different x_i , it will take them a long time to get out of that bad region.

As an illustration, consider the additive lagged-Fibonacci generator based on the recurrence $x_i = (x_{i-21034} + x_{i-44497}) \bmod 2^{32}$, available in The Boost C++ Library (Maurer and Watanabe 2010), and which behaves just like the $DX-k-1-t$ generator with $b = 1$ and $k = 44497$. If we initialize this generator with $x_i = c$ for $i = -k + 1, \dots, 0$, the first 21034 output values are all equal to $2c \bmod m$; then the next 21034 output values are all equal to $3c \bmod m$, and it takes a huge number of steps before this structure dissipates. We used this initialization with $c = 123456789$; we generated and discarded 2^{29} (nearly one billion) random numbers from the generator, and then applied a birthday spacings test with sample size $n = 2^{11}$, with 2^{28} cells in two dimensions. The generator failed the test with a p -value smaller than 10^{-300} .

As another example, consider the SWB proposed in Marsaglia (1999), based on the recurrence $x_i = (x_{i-222} - x_{i-237} - b_{i-1}) \bmod 2^{32}$ with borrow $b_i = \mathbb{I}[x_{i-222} < x_{i-237} + b_{i-1}]$, where \mathbb{I} is the indicator function. If we initialize this generator with $x_i = 123456789$ for $i = -236, \dots, 0$ and $b_0 = 0$, then among the first 1000 values x_1, \dots, x_{1000} , 466 are 0 and 384 are 1. If we

then generate and discard 2^{13} values and then apply a birthday spacings test with sample size $n = 2^{11}$, with 2^{28} cells in $d = 2$ dimensions, the generator fails the test with a p -value smaller than 10^{-300} (the number of observed collisions is 693 compared with an expected number of eight).

6. Conclusion

We have examined structural properties of special classes of MRGs designed to have a very long period and a fast implementation. We found that the points produced by these generators have a lot of structure. In particular, low-dimensional points constructed from output values at certain specific lags have a poor lattice structure, regardless of the choice of parameters within certain classes of MRGs. A naive initialization of the state can also produce very bad and long-lasting behavior in the output, because of the limited diffusion capacity of the recurrence. This behavior happens when the recurrence has large order k , and there are too few nonzero coefficients a_j , or all (or most) of these coefficients are equal to the same value b . It is particularly bad when the smallest lag in the recurrence (e.g., the value of t for a $DX-k-\sigma-t$ generator) is large.

This type of behavior tilts the balance against MRGs with very large order k . Other arguments are that MRGs with large order k have a very large state, which means more overhead for the initialization and even more overhead to maintain multiple streams and substreams of random numbers for parallel processing and for comparing systems with well-synchronized common random numbers (L'Ecuyer et al. 2002). Jumping ahead in the sequence to produce disjoint streams and substreams becomes too slow when k is large. Recurrences of smaller order k having both a fast implementation and a high diffusion capacity are easy to construct (L'Ecuyer 1999a) and

provide random numbers with sufficiently good quality for practically all current simulation applications.

Acknowledgments

The authors thank the three reviewers and the Associate Editor Marvin Nakayama, whose comments and suggestions led to a better paper. Alexandru Ionut had contributed to an earlier version of this paper, but then refused to be a co-author, so the authors removed his contribution. They nevertheless thank him for his earlier help. This work has been supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada, an Equipment Grant from the Canadian Fund for Innovation, and a Canada Research Chair, to Pierre L'Ecuyer.

References

- Conway JH, Sloane NJA (1999) *Sphere Packings, Lattices and Groups* 3rd ed. Grundlehren der Mathematischen Wissenschaften 290, (Springer-Verlag, New York).
- Deng L-Y (2004) Generalized Mersenne prime number and its application to random number generation. Niederreiter H, ed. *Monte Carlo and Quasi-Monte Carlo Methods 2002* (Springer-Verlag, Berlin), 167–180.
- Deng L-Y (2005) Efficient and portable multiple recursive generators of large order. *ACM Trans. Modeling Comput. Simulation* 15:1–13.
- Deng L-Y (2008) Issues on computer search for large-order multiple recursive generators. Keller A, Heinrich S, Niederreiter H, eds. *Monte Carlo and Quasi-Monte Carlo Methods 2006* (Springer-Verlag, Berlin), 251–261.
- Deng L-Y, Lin DKJ (2000) Random number generation for the new century. *Amer. Statistician* 54:145–150.
- Deng L-Y, Xu H (2003) A system of high-dimensional, efficient, long-cycle and portable uniform random number generators. *ACM Trans. Modeling Comput. Simulation* 13:299–309.
- Deng L-Y, Li H, Shiau J-JH (2009) Scalable parallel multiple recursive generators of large order. *Parallel Comput.* 35:29–37.
- Deng L-Y, Shiau J-JH, Lu HH-S (2012) Large-order multiple recursive generators with modulus $2^{31} - 1$. *INFORMS J. Comput.* 24:636–647.
- Deng L-Y, Li H, Shiau J-JH, Tsai GH (2008) Design and implementation of efficient and portable multiple recursive generators with few zero coefficients. Keller A, Heinrich S, Niederreiter H, eds. *Monte Carlo and Quasi-Monte Carlo Methods 2006* (Springer-Verlag, Berlin), 263–273.
- Knuth DE (1998) *The Art of Computer Programming, Volume 2: Semi-numerical Algorithms*, 3rd ed. (Addison-Wesley, Reading, MA).
- L'Ecuyer P (1997) Bad lattice structures for vectors of non-successive values produced by some linear recurrences. *INFORMS J. Comput.* 9:57–60.
- L'Ecuyer P (1999a) Good parameters and implementations for combined multiple recursive random number generators. *Oper. Res.* 47:159–164.
- L'Ecuyer P (1999b) Tables of maximally equidistributed combined LFSR generators. *Math. Comput.* 68:261–269.
- L'Ecuyer P (2006) Uniform random number generation. Henderson SG, Nelson BL, eds. *Simulation. Handbooks in Operations Research and Management Science*, Chap. 3 (Elsevier, Amsterdam), 55–81.
- L'Ecuyer P, Couture R (1997) An implementation of the lattice and spectral tests for multiple recursive linear random number generators. *INFORMS J. Comput.* 9:206–217.
- L'Ecuyer P, Simard R (2001) On the performance of birthday spacings tests for certain families of random number generators. *Math. Comput. Simulation* 55:131–137.
- L'Ecuyer P, Simard R (2007) TestU01: A C library for empirical testing of random number generators. *ACM Trans. Math. Software* Vol. 33, Article 22.
- L'Ecuyer P, Touzin R (2000) Fast combined multiple recursive generators with multipliers of the form $a = \pm 2^q \pm 2^r$. Joines JA, Barton RR, Kang K, Fishwick PA, eds. *Proc. 2000 Winter Simulation Conf.* (IEEE Press, Piscataway, NJ), 683–689.
- L'Ecuyer P, Touzin R (2004) On the Deng-Lin random number generators and related methods. *Statist. Comput.* 14:5–9.
- L'Ecuyer P, Simard R, Chen EJ, Kelton WD (2002) An object-oriented random-number package with many long streams and substreams. *Oper. Res.* 50:1073–1075.
- Marsaglia G (1985) A current view of random number generators. Billard L, ed. *Comput. Sci. Statist., Sixteenth Sympos. Interface* (Elsevier Science Publishers, North-Holland, Amsterdam), 3–10.
- Marsaglia G (1999) Random numbers for C: The END? Posted to the electronic billboard sci.math.num-analysis. <https://groups.google.com/forum/#!search/marsaglia%20random%20numbers%20222/sci.math.num-analysis/yoaCpGWKEk0/UXCygufdTesJ>.
- Matsumoto M, Wada I, Kuramoto A, Ashihara H (2007) Common defects in initialization of pseudorandom number generators. *ACM Trans. Modeling Comput. Simulation* Vol. 17, Article 15.
- Maurer J, Watanabe S (2010) Boost random number library. <http://www.boost.org/libs/random/index.html>.
- Niederreiter H (1992) *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM CBMS-NSF Regional Conf. Ser. Appl. Math., Vol. 63 (SIAM, Philadelphia).
- Sós VT (1958) On the distribution mod 1 of the sequence na . *Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Math.* 1:127–134.
- van Ravenstein T (1988) The three gap theorem (Steinhaus conjecture). *J. Australian Math. Soc., Ser. A* 45:360–370.