Les cahiers du GERAD ISSN: 0711-2440

Structural Properties for Two Classes of Combined Random Number Generators

P. L'Ecuyer, S. Tezuka

G–90–56

December 1990

Structural Properties for Two Classes of Combined Random Number Generators

Pierre L'Ecuyer
Département d'IRO, Université de Montréal,
C.P. 6128, Succ. A, Montréal
Canada, H3C 3J7

Shu Tezuka
IBM Research, Tokyo Research Laborator
5-19, Sanbancho, Chiyodaku, Tokyo 10
JAPAN

November 1990

Abstract

We analyze a class of combined random number generators proposed by L'Ecuyer (1988), which combines a set of linear congruential generators (LCGs) with distinct prime moduli. We show that the geometrical behavior of the vectors of points produced by the combined generator can be approximated by the lattice structure of an associated LCG, whose modulus is the product of the moduli of the individual components. The approximation is good if these individual moduli are near each other and if the dimension of the vectors is large enough. The associated LCG is also exactly equivalent to a slightly different combined generator, of the form suggested by Wichmann and Hill (1982). We give illustrations, for which we examine the approximation error and assess the quality of the lattice structure of the associated LCG.

KEYWORDS: Rrandom number generation; lattice structure; combined generators; Chinese Remainder Theorem

Résumé

Nous analysons une classe de générateurs de valeurs aléatoires proposés par L'Ecuyer (1988), combinant un ensemble de générateurs à congruence linéaire (LCG) avec des modulos premiers distincts. Nous montrons que la disposition géométrique des vecteurs de points produits par le générateur combiné peut être approximée par la structure de treillis d'un LCG unique associé, dont le modulo est égal au produit des modulos des générateurs que l'on combine. L'approximation sera bonne si ces modulos individuels sont proches les uns des autres et si la dimension des vecteurs est assez grande. Le LCG associé est aussi exactement equivalent à un générateur combiné légèrement différent, du type de celui suggéré par Wichmann et Hill (1982). Nous illustrons le tout par des exemples pour lesquels nous examinons l'erreur d'approximation et évaluons la qualité de la structure de treillis du LCG associé.

1. Approximating a Combined Generator by a LCG

Consider J LCGs ($J \geq 2$) such that for $j = 1, \ldots, J$, generator j has modulus m_j and multiplier a_j. Suppose that the m_j's are all distinct primes and that each LCG has maximal period $m_j - 1$ (a_j is a primitive element modulo m_j). Let s_{ji} denote the state of generator j at step i, that is

$$s_{ji} := a_j s_{j,i-1} \bmod m_j. \tag{1}$$

Let $\delta_1, \ldots, \delta_J$ be arbitrary non-zero integers. Define the two combined generators

$$Z_i = \left(\sum_{j=1}^{J} \delta_j s_{ji} \right) \bmod m_1; \qquad U_i = Z_i / m_1 \tag{2}$$

and

$$W_i = \left(\sum_{j=1}^{J} \delta_j s_{ji}/m_j \right) \bmod 1. \tag{3}$$

The former is suggested in [5] (with $\delta_j = (-1)^{j-1}$, for ease of implementation), while the latter generalizes Wichmann and Hill [11]. Let

$$n_j = (m/m_j)^{m_j - 2} \bmod m_j \qquad \text{for } j = 1, \ldots, J; \tag{4}$$

$$m = \prod_{j=1}^{J} m_j \; ; \tag{5}$$

$$a = \left(\sum_{j=1}^{J} a_j n_j m/m_j \right) \bmod m \; ; \tag{6}$$

and define the LCG (with composite modulus):

$$Y_i := a Y_{i-1} \bmod m; \qquad \tilde{U}_i = Y_i / m. \tag{7}$$

In Proposition 1 below, we show that the combined generator (3) is equivalent to the LCG (7). This is related to the Chinese Remainder Theorem and means that (3) is in fact an implementation of (7) using modular arithmetic [4, §4.3.2]. An alternative approach for computing a is also given in [4, p. 274]. In Proposition 2, we show that if the m_j's are near each other, generator (2) is approximately equivalent to (7) and (3), with some added "noise". We give tight bounds on the noise. This approximation is valid under the assumption that to produce $U(0,1)$ variates, the generator's state is simply divided by the modulus, as in (2) and (7). These results were derived in [9] for the special case $J = 2$ and $\delta_1 = \delta_2 = 1$. Note that a and m do not depend on the δ_j's. A corollary to Proposition 1 is that the period length of (3) is equal to the Carmichael's function $\lambda(m)$, which in this case is equal to the least common multiple of $m_1 - 1, \ldots, m_J - 1$.

PROPOSITION 1. *If $Y_0/m = W_0$, then $\tilde{U}_i = Y_i/m = W_i$ for all $i \geq 0$.*

PROOF. From the definition of n_j and from Fermat's little Theorem (see, e.g., [8]), one has

$$n_j(m/m_j) \bmod m_j = (m/m_j)^{m_j-1} \bmod m_j = 1 \tag{8}$$

so that $n_j m/m_j = 1 + Km_j$ for some integer K and

$$n_j(m/m_j)^2 \bmod m = (m/m_j)(1 + Km_j) \bmod m = m/m_j.$$

From this and since $(m/m_k)(m/m_j) \bmod m = 0$ for $k \neq j$, one gets

$$\begin{aligned}
amW_i \bmod m &= \left(\sum_{k=1}^{J} a_k n_k m/m_k\right)\left(\sum_{j=1}^{J} m\delta_j s_{ji}/m_j\right) \bmod m \\
&= \left(\sum_{j=1}^{J} n_j(m/m_j)^2 a_j \delta_j s_{ji}\right) \bmod m \\
&= \left(\sum_{j=1}^{J} (m/m_j)\delta_j a_j s_{ji}\right) \bmod m \\
&= \left(\sum_{j=1}^{J} (m/m_j)\delta_j (a_j s_{ji} \bmod m_j)\right) \bmod m \\
&= mW_{i+1}.
\end{aligned}$$

Therefore, mW_i satisfies the recursion (7), the same as Y_i. ∎

COROLLARY 1. *The period of (3) (and (7)) is always equal to $\lambda(m)$, provided that for all j, we have $(\delta_j \bmod m_j) \neq 0$ and $(s_{j0} \bmod m_j) \neq 0$.*

PROOF. It suffices to show that $Y_0 = mW_0$ is prime to m and that a is a primitive element modulo m, and the result will follow from Carmichael's Theorem [4, §3.2.1.2]. Under the assumption of the corollary, since m_j is prime, $\delta_j s_{j0} m/m_j$ is prime to m_j, and $mW_0 = \sum_{k=1}^{J} \delta_k s_{k0} m/m_k$ too, because in this sum, all terms with indexes $k \neq j$ are multiples of m_j. Since this holds for all j, mW_0 is prime to all prime factors of m, that is prime to m. Saying that a is a primitive element modulo m means that there is no positive integer k smaller than $\lambda(m)$ such that $a^k \bmod m = 1$. If such a k exists, then $a_j^k \bmod m_j = a^k \bmod m_j = 1$ because $a \bmod m_j = (a_j n_j m/m_j) \bmod m_j = a_j$ from (8). But since a_j is a primitive element modulo m_j, k must be a multiple of $\lambda(m_j) = m_j - 1$. Since this holds for all j, k must be a multiple of $\lambda(m)$. ∎

Here, the period of (7) is much smaller than $m - 1$ (for $J \geq 2$) because the set of states $\{1, \ldots, m-1\}$ is partitioned into subcycles. Of course, it is possible to recover the full period by juxtaposing or interleaving the subcycles. But this complicates the implementation and does not appear to be really helpful in practice.

Define

$$\begin{aligned}
\Psi^+ &= \{j \mid 2 \leq j \leq J \text{ and } (m_j - m_1)\delta_j > 0\} \\
\Psi^- &= \{j \mid 2 \leq j \leq J \text{ and } (m_j - m_1)\delta_j < 0\}
\end{aligned}$$

$$\begin{aligned}
\Delta^+ &= \sum_{j\in\Psi^+} \frac{(m_j - m_1)(m_j - 1)\delta_j}{m_1 m_j} + \sum_{j\in\Psi^-} \frac{(m_j - m_1)\delta_j}{m_1 m_j} \\
\Delta^- &= \sum_{j\in\Psi^+} \frac{(m_j - m_1)\delta_j}{m_1 m_j} + \sum_{j\in\Psi^-} \frac{(m_j - m_1)(m_j - 1)\delta_j}{m_1 m_j} \\
\Delta &= \max(|\Delta^+|, |\Delta^-|).
\end{aligned}$$

PROPOSITION 2. *If $Y_0/m = W_0$, then*

$$U_i = (W_i + \epsilon_i) \bmod 1 \tag{9}$$

where

$$\Delta^- \le \epsilon_i \le \Delta^+. \tag{10}$$

PROOF. For some integer K, one has

$$\begin{aligned}
Z_i &= \left(\sum_{j=1}^{J} [(m/m_j)(m_1/m) + 1 - (m_1/m_j)]\, \delta_j s_{ji} \right) \bmod m_1 \\
&= \left((m_1/m)(Y_i + Km) + \sum_{j=1}^{J} \left(1 - \frac{m_1}{m_j}\right) \delta_j s_{ji} \right) \bmod m_1 \\
&= (m_1 Y_i/m + m_1 \epsilon_i) \bmod m_1
\end{aligned}$$

where

$$m_1 \epsilon_i = \sum_{j=1}^{J} \left(1 - \frac{m_1}{m_j}\right) \delta_j s_{ji} = \sum_{j=2}^{J} \frac{(m_j - m_1)\delta_j s_{ji}}{m_j}.$$

Dividing by m_1 and since $1 \le s_{ij} \le m_j - 1$ for all j, (9) and (10) follow easily. ∎

Note that the bounds on ϵ_i are tight, since $\epsilon_i = \Delta^+$ [$\epsilon_i = \Delta^-$] (respectively) when $s_{ji} = m_j - 1$ for $j \in \Psi^+$ [for $j \in \Psi^-$] and $s_{ji} = 1$ for $j \in \Psi^-$ [for $j \in \Psi^+$]. For example, let $J = 2$, $\delta_1 = 1$, $\delta_2 = -1$, and $m_1 > m_2$. Then, $\Psi^+ = \{2\}$, Ψ^- is empty, $\Delta^+ = (m_1 - m_2)(m_2 - 1)/(m_1 m_2)$, $\Delta^- = (m_1 - m_2)/(m_1 m_2)$, and $\epsilon_i = (m_1 - m_2)s_{2i}/(m_1 m_2)$. We have $\epsilon_i = \Delta^+$ when $s_{2i} = m_2 - 1$ and $\epsilon_i = \Delta^-$ when $s_{2i} = 1$.

From now on, assume that $Y_i/m = W_i$. It is well known [3, 4] that all t-tuples of successive values $\{\tilde{P}_i^t = (\tilde{U}_i, \ldots, \tilde{U}_{i+t-1}) = (W_i, \ldots, W_{i+t-1}) \in [0,1)^t,\ i \ge 0\}$ lie on a lattice $\tilde{L}_t$. Different "figures of merit", relative to the geometrical properties of $\tilde{L}_t$, can be computed for "rating" the corresponding LCG. Among them are the Beyer quotient $q_t \in (0,1]$ and the distance d_t between successive hyperplanes covering the points [2, 4, 3]. It is traditionally accepted that q_t should be near one for all values of t up to a certain constant T (or for which q_t can be computed). But the generator's quality also depends strongly on the modulus. As argued in [7], a generator with larger modulus (or of higher order), even if it has a smaller q_t, might be better. A good "bottom of the line" criterion is in fact the distance d_t between hyperplanes. Reducing d_t in all dimensions t should be considered as an improvement.

Note that for $J \geq 2$, the t-tuples $\tilde{P}_i^t$ form a *strict* subset of the lattice points in $[0,1)^t$, since generator (7) *does not* have maximal period (m is not prime). But if we take all t-tuples of successive values produced by all subcycles of the generator, then this set of points is $\tilde{L}_t \cap [0,1)^t$ for some lattice $\tilde{L}_t$, and this is the lattice that we analyze in this paper. In all the examples that we have examined, $\tilde{L}_t$ was also the smallest lattice spanned by the points $\tilde{P}_i^t$ over one of the subcycles that could be used.

The points $\{P_i^t = (U_i, \ldots, U_{i+t-1}),\ i \geq 0\}$ do not belong in general to $\tilde{L}_t$. But we see from Proposition 2 that the Euclidean distance between P_i^t and $\tilde{P}_i^t$ obeys

$$\|P_i^t - \tilde{P}_i^t\| \leq (\epsilon_i^2 + \cdots + \epsilon_{i+t-1}^2)^{1/2} \leq \Delta\sqrt{t}. \tag{11}$$

(To take into account the mod 1 operation, consider all the t-dimensional unit hypercubes with integer vertices. Each one contains a "representative" of P_i^t, whose coordinates are the same as P_i^t, modulo one. Redefine $\|P_i^t - \tilde{P}_i^t\|$ as the Euclidean distance between $\tilde{P}_i^t$ and the nearest representative of P_i^t.) When $\Delta\sqrt{t}$ is much smaller than d_t, the combined generator has *approximately* the same hyperplane structure as its associate LCG. To get rid (to some extent) of the lattice structure (at least in smaller dimensions), one should get a larger Δ. This can be achieved by increasing the values of $|\delta_j(m_j - m_1)|$. We remark that $\Delta\sqrt{t}$ is just an upper bound. However, for all the examples that we have examined, that bound was always attained (or almost attained) for some i.

2. The Approximate Lattice Structure for Some Examples

Example 1

Let $J = 2$, $m_1 = 101$, $m_2 = 97$, $a_1 = 51$, $a_2 = 58$, $\delta_1 = 1$ and $\delta_2 = -1$. Equations (2) and (3) become respectively $Z_i = (s_{1i} - s_{2i}) \bmod 101$ and $W_i = (s_{1i}/101 - s_{2i}/97) \bmod 1$, which have period 2400. One obtains $m = 9797$, $n_1 = (97^{99} \bmod 101) = 25$, $n_2 = (101^{95} \bmod 97) = 73$, $a = (a_1 n_1 m_2 + a_2 n_2 m_1) \bmod m = 2677$, $\Delta^- \approx .0004$ and $\Delta = \Delta^+ \approx .0392$. The associated LCG is then

$$Y_i = 2677 Y_{i-1} \bmod 9797. \tag{12}$$

Pairs of successive values are plotted in Figures 1–4 for the two combined generators and the two individual components. The latter have small periods and coarse lattice structures. The lattice structure of the LCG (12), which corresponds to the W_i's, is also apparent in two dimensions. Although it is certainly not to be recommended, this generator is nevertheless an improvement over each (much smaller) individual component. The plot for the other combination (the U_i's, in Figure 4) looks a little better. The lines of Figure 3 are no more apparent. In fact, the distance between adjacent lines in Figure 3 is 0.0175, while the bound in (11) is $\Delta\sqrt{2} \approx 0.0554$. The resolution along each axis is smaller in Figure 4 than in Figure 3: all U_i's are multiples of $1/m_1$, while the W_i's are multiples of $1/m$, which is much smaller. This is why, in Figure 4, the points lie on easily discernable equidistant vertical lines, and also on equidistant horizontal lines.

Table 1: Results for the LCGs of Example 1.

	(m, a)			(m_1, a_1)	(m_2, a_2)
t	q_t	d_t	$\Delta\sqrt{t}$	d_t	d_t
2	.3305	.0175	.0554	.447	.196
3	.2479	.0953	.0679	.447	.218
4	.7597	.1111	.0784	.447	.377
5	.6362	.1925	.0876	.447	.500
6	.8029	.2182	.0960	.447	.500
7	.7395	.2887	.1037	.500	.500
8	.5671	.4472	.1109	.500	.500
9	.5731	.4472	.1176	.500	.577
10	.6400	.4472	.1239	.577	.577
11	.6417	.4472	.1300	.577	.577
12	.7468	.4472	.1358	.577	.577

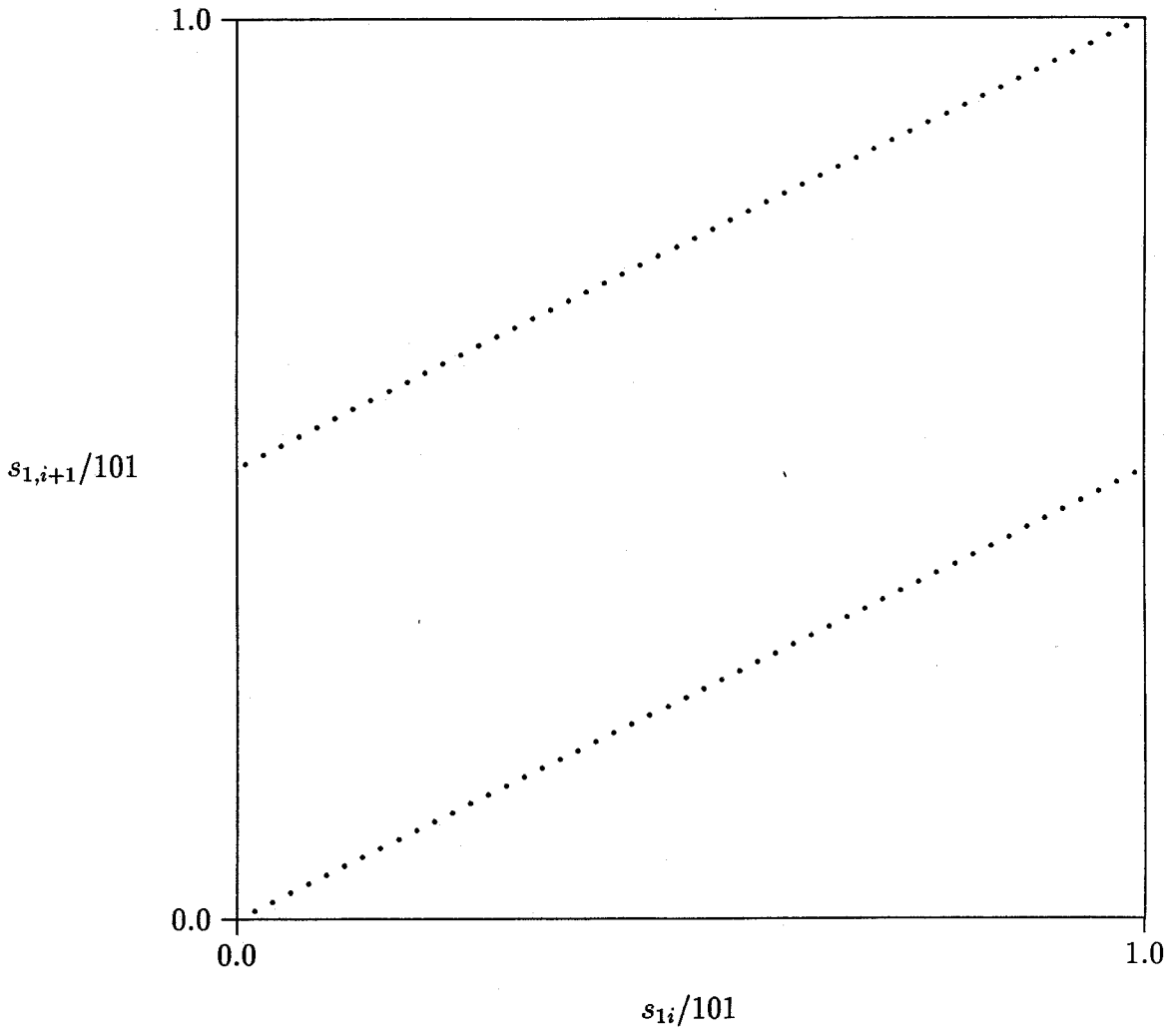

Figure 1. All pairs of successive points for the LCG with $m = 101$ and $a = 51$.

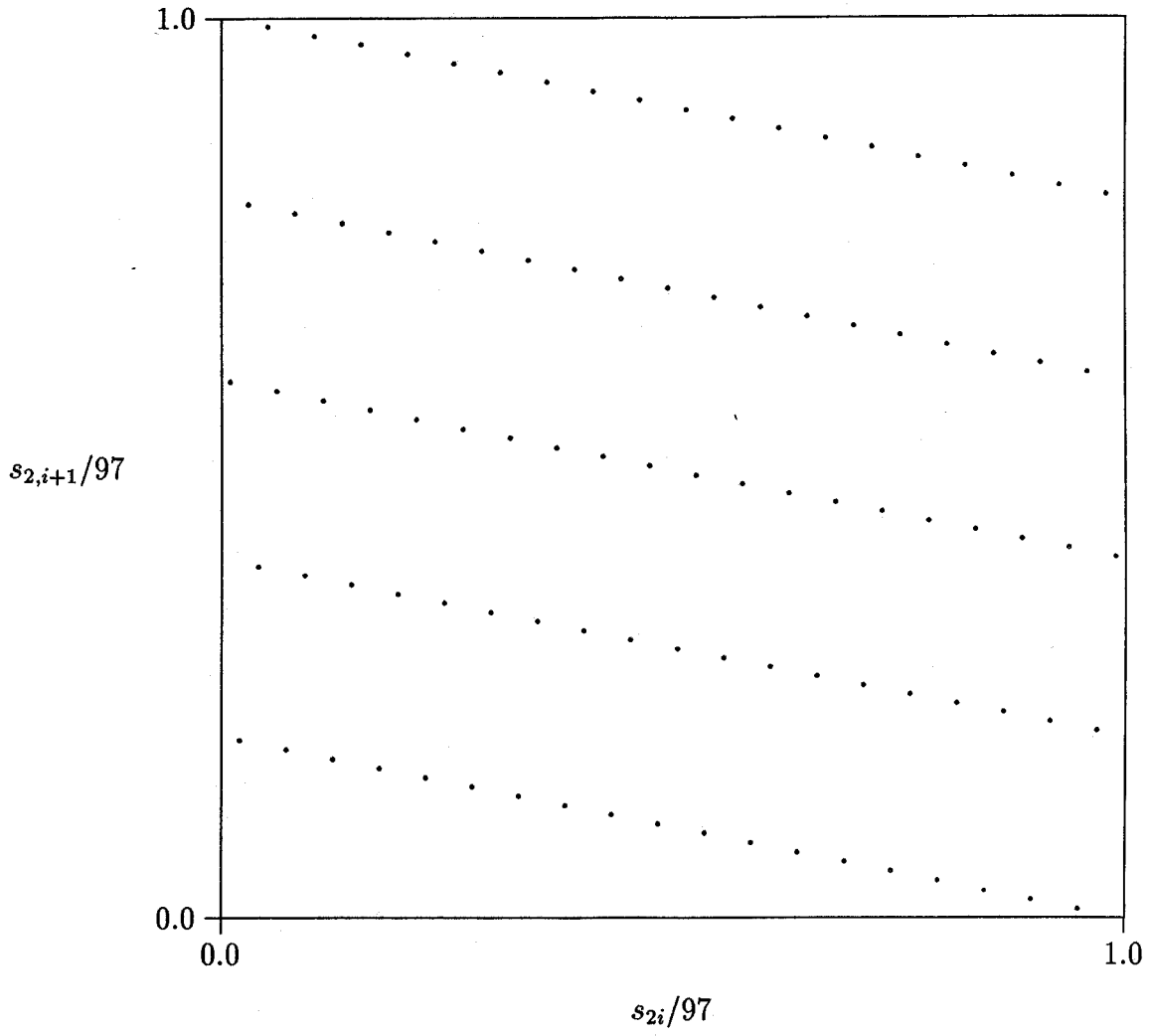

Figure 2. All pairs of successive points for the LCG with $m = 97$ and $a = 58$.

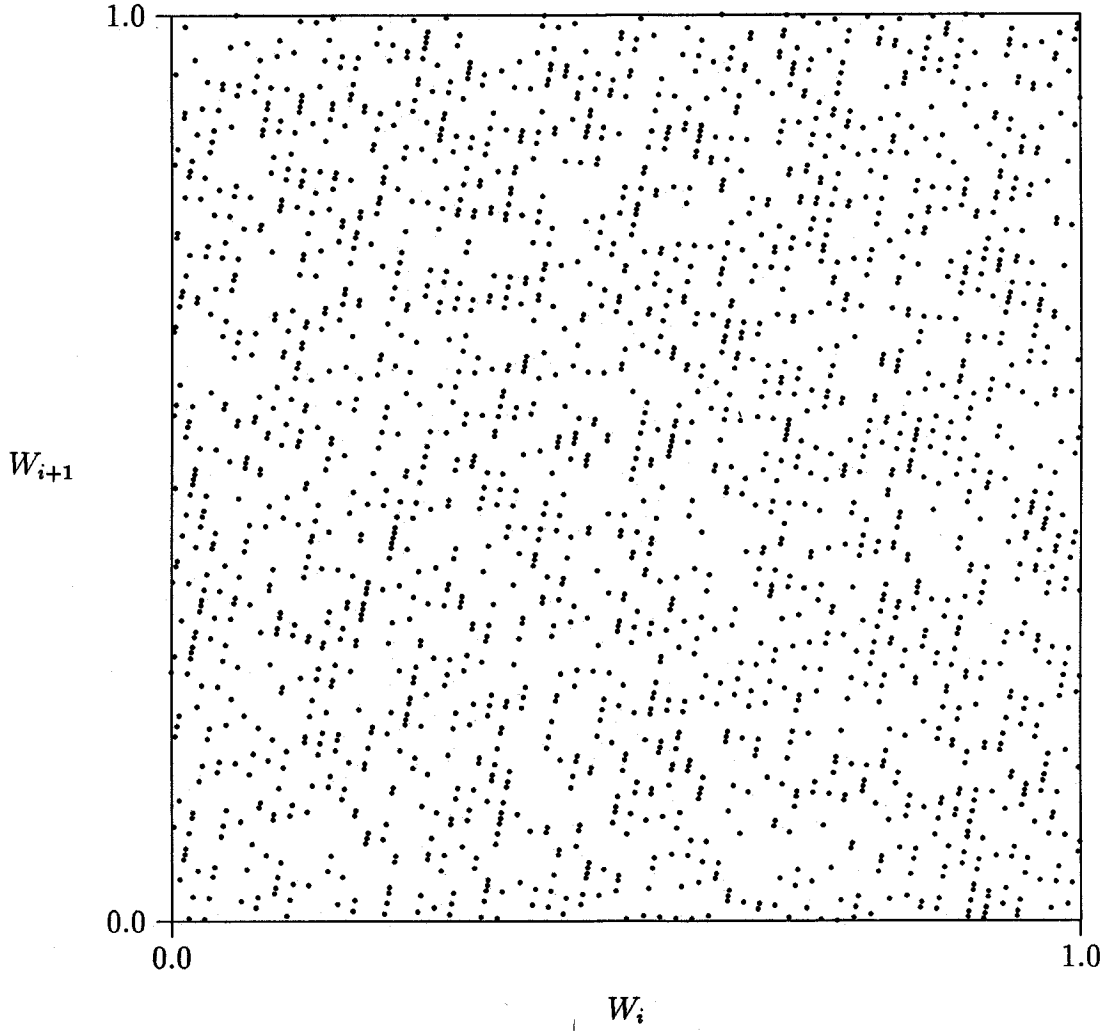

Figure 3. Pairs of successive points for the LCG with $m = 9797$ and $a = 2677$.

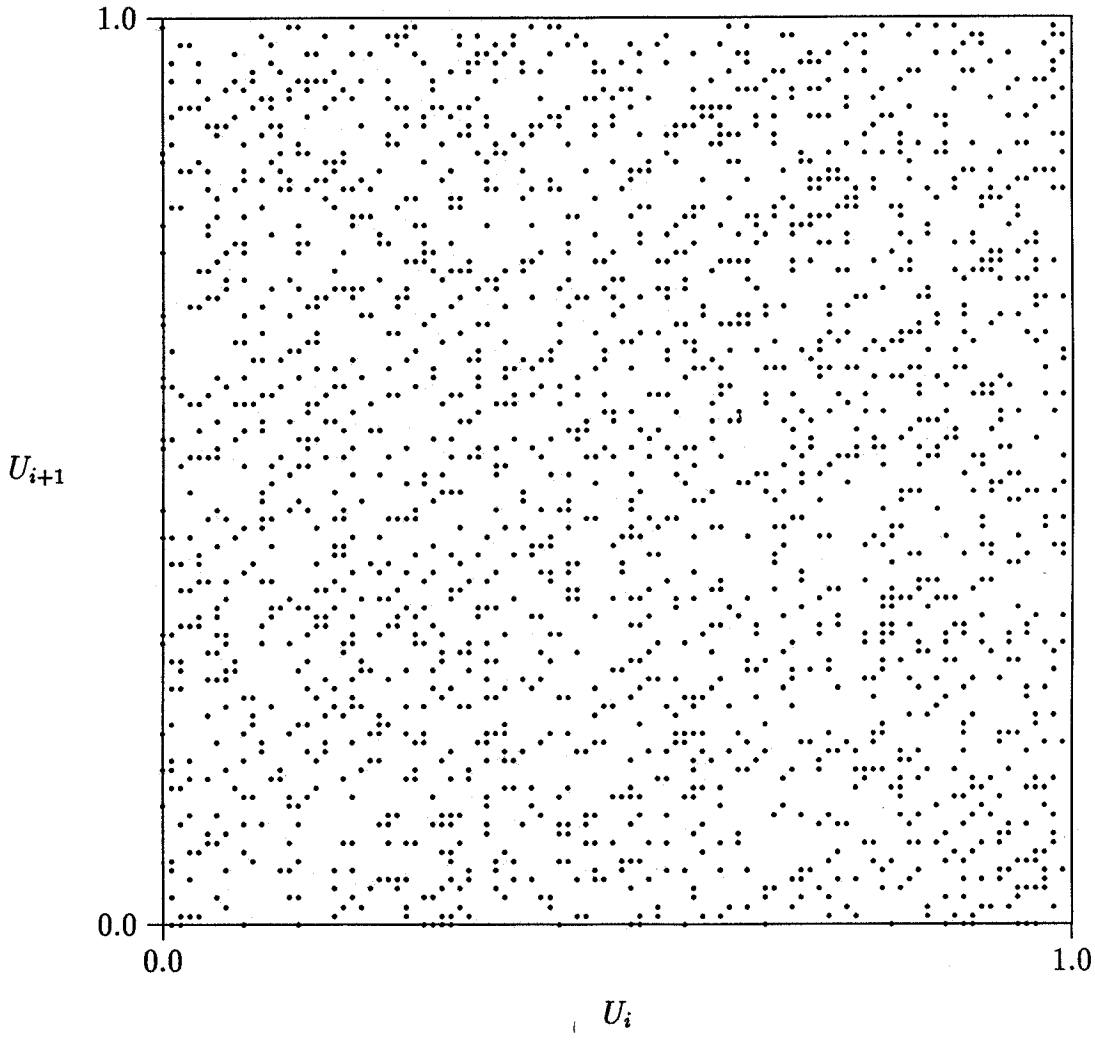

Figure 4. Pairs of successive points for the combined generator $U_i = ((s_{1i} - s_{2i}) \bmod 101)/101$.

In higher dimensions, the distance between hyperplanes typically gets larger, often significantly larger than Δ. In Table 1, we give the Beyer quotients q_t, distances d_t between hyperplanes, and values of $\Delta\sqrt{t}$ for the LCG (12), for $t \leq 12$. For comparison, we also give the values of d_t for the individual LCG components. These quantities were computed using (with some adaptations) the algorithm described in [1].

Example 2

One combined generator suggested in [5] has $J = 2$, $m_1 = 2147483563$, $m_2 = 2147483399$, $a_1 = 40014$, $a_2 = 40692$, $\delta_1 = 1$, and $\delta_2 = -1$. In this case, one has $m = 4611685301167870637$, $n_1 = 1715367968$, $n_2 = 432115562$, $a = 1968402271571654650$, $\Delta^- \approx 3.5 \times 10^{-17}$, and $\Delta = \Delta^+ \approx 7.637 \times 10^{-8}$. The combined generator (2), as well as its associated LCG $Y_i = aY_{i-1} \bmod m$, have period length of $(m_1 - 1)(m_2 - 1)/2 = 2.306 \times 10^{18}$. Table 2 gives similar information as Table 1, for this second example. One can see that in high dimensions, the "noise" $\Delta\sqrt{t}$ becomes very small with respect to the distance between hyperplanes. This was already noticed by Tezuka [9]. On the other hand, the hyperplane structure of the associated LCG is much better than for any of its components, and much better than for any LCG with modulus smaller than 2^{31}. This is true despite its bad Beyer quotient in dimension 4. That combined generator has essentially the properties of a LCG with larger modulus m and can be implemented efficiently without getting into the trouble of dealing with large integers (of more than 31 bits). As we will see in Example 4, for the same size, one can also find better combined generators than this one.

Table 2: The 32-bit combined generator of L'Ecuyer [5].

	(m, a)			(m_1, a_1)	(m_2, a_2)
t	q_t	d_t	$\Delta\sqrt{t}$	d_t	d_t
2	.5009	6.50E-10	1.08E-7	2.499E-5	2.457E-5
3	.7016	7.002E-7	1.32E-7	8.263E-4	8.441E-4
4	.1443	4.635E-5	1.53E-7	4.954E-3	4.852E-3
5	.5975	2.008E-4	1.71E-7	1.334E-2	1.240E-2
6	.6173	8.890E-4	1.87E-7	2.670E-2	2.637E-2
7	.6130	2.621E-3	2.02E-7	7.274E-2	7.274E-2
8	.5737	5.782E-3	2.16E-7	7.274E-2	7.274E-2
9	.5589	9.571E-3	2.29E-7	9.806E-2	8.737E-2
10	.5532	1.738E-2	2.41E-7	1.474E-1	1.054E-1
11	.6390	2.361E-2	2.53E-7	1.474E-1	1.324E-1
12	.6635	3.077E-2	2.64E-7	1.474E-1	1.443E-1

Example 3

Wichmann and Hill [11] originally suggested a combination of the form (3), with $J = 3$, $m_1 = 30269$, $m_2 = 30307$, $m_3 = 30323$, $a_1 = 171$, $a_2 = 172$, $a_3 = 170$, and $\delta_1 = \delta_2 = \delta_3 = 1$. This

yields $m = 27817185604309$, $n1 = 26478$, $n2 = 26070$, $n3 = 8037$, and $a = 16555425264690$. The equivalence of this generator to a LCG was first pointed out by Zeisel [12]. If one uses Equation (2) with these values, one also gets $\Delta^- \approx -.00125$ and $\Delta = \Delta^+ \approx .00178$. L'Ecuyer [5] gave a different one, of the form (2), with $J = 3$, $m_1 = 32363$, $m_2 = 31727$, $m_3 = 31657$, $a_1 = 157$, $a_2 = 146$, $a_3 = 142$, and $\delta_1 = -\delta_2 = \delta_3 = 1$. In that case, one has $m = 32504802982957$, $n1 = 29617$, $n2 = 17633$, $n3 = 16749$, $a = 30890646900944$, $\Delta^+ \approx .0196$, and $\Delta = -\Delta^- \approx .00218$. These generators have respective periods of (approximately) 6.95×10^{12} and 8.12×10^{12}. Tables 3 and 4 give other information on them and on their components. The associated LCG of the second combined generator is bad in dimensions 2 and 6 compared to the first one. But note that even if q_2 is small, d_2 is nevertheless smaller in this case than for any standard LCG with modulus $m = 2^{31} - 1$. Also, the added noise is significantly larger than the distance between hyperplanes, at least up to dimension 12. The hyperplane structure is lost in the noise. On the other hand, the resolution is only $1/m_1$, which means that all points lie on vertical lines that are $1/32363$ apart (and the same horizontally). For this reason, perhaps this generator should not be recommended too strongly for serious applications.

Table 3: The combined generator of Wichmann and Hill [11].

	(m, a)			(m_1, a_1)	(m_2, a_2)	(m_3, a_3)
t	q_t	d_t	$\Delta\sqrt{t}$	d_t	d_t	d_t
2	.6371	2.370E-7	.0025	.0058	.0058	.0058
3	.4842	4.428E-5	.0031	.1562	.0459	.0419
4	.7084	5.418E-4	.0036	.1562	.0905	.1374
5	.8313	2.076E-3	.0040	.1562	.1313	.1374
6	.7275	6.328E-3	.0044	.1690	.1768	.2294
7	.4582	1.690E-2	.0047	.3536	.2425	.2294
8	.7190	2.478E-2	.0050	.3536	.3333	.3333
9	.8083	2.993E-2	.0054	.3536	.3333	.3333
10	.7242	4.588E-2	.0056	.3536	.3333	.3333
11	.7422	5.987E-2	.0059	.3536	.3333	.3780
12	.7185	7.255E-2	.0062	.4472	.4082	.3780

Table 4: The 16-bit combined generator of L'Ecuyer [5].

	(m, a)			(m_1, a_1)	(m_2, a_2)	(m_3, a_3)
t	q_t	d_t	$\Delta\sqrt{t}$	d_t	d_t	d_t
2	.0181	1.304E-6	.0308	.0064	.0068	.0070
3	.6209	4.184E-5	.0378	.0329	.0390	.0369
4	.6868	4.638E-4	.0436	.0758	.0867	.0765
5	.6003	2.069E-3	.0487	.1302	.1348	.1302
6	.2368	1.357E-2	.0534	.1741	.1890	.1768
7	.6617	1.357E-2	.0577	.2887	.2500	.2582
8	.4987	3.176E-2	.0617	.2887	.3536	.2774
9	.5420	3.328E-2	.0654	.4082	.3536	.2887
10	.7849	4.921E-2	.0690	.4082	.3536	.3780
11	.7711	5.670E-2	.0723	.4082	.3536	.3780
12	.8363	6.523E-2	.0756	.4472	.3536	.3780

Example 4

We now give an example of a combined generator of roughly the same size as Example 2, whose associated LCG has a lattice structure of slightly better quality, and with much more noise. Incidentally, its two LCG components have bad lattice structures in dimension 3. The first one has $q_3 = .0167$ and the second one has $q_3 = .1022$. One has $J = 2$, $m_1 = 2147483647$, $m_2 = 2145483479$, $a_1 = 26756$, $a_2 = 30318$, $\delta_1 = 1$, and $\delta_2 = -1$. In this case, one has $m = 4607390686061167913$, $n_1 = 1317463960$, $n_2 = 829246600$, $a = 3416908681540390868$, $\Delta^- \approx 4.34 \times 10^{-13}$, and $\Delta = \Delta^+ \approx 9.314 \times 10^{-4}$. The combined generator (2) and its associated LCG (7) have period length of $(m_1 - 1)(m_2 - 1)/2 \approx 2.30 \times 10^{18}$. Table 5 gives further information. Up to dimension 7, there could be enough noise to mask the hyperplane structure. Also, the smallest Beyer quotient is larger here than for Example 2.

Table 5: A new 32-bit combined generator.

t	(m, a) q_t	d_t	$\Delta\sqrt{t}$	(m_1, a_1) d_t	(m_2, a_2) d_t
2	.6934	5.54E-10	1.32E-3	3.738E-5	3.298E-5
3	.7979	6.379E-7	1.61E-3	5.138E-3	2.986E-3
4	.8388	2.156E-5	1.86E-3	5.138E-3	5.717E-3
5	.9328	1.737E-4	2.08E-3	1.724E-2	1.623E-2
6	.8074	7.731E-4	2.28E-3	4.046E-2	3.400E-2
7	.5380	2.384E-3	2.46E-3	4.730E-2	5.184E-2
8	.7447	4.996E-3	2.63E-3	7.495E-2	8.909E-2
9	.7727	9.720E-3	2.79E-3	1.072E-1	8.909E-2
10	.6280	1.266E-2	2.95E-3	1.104E-1	1.361E-1
11	.7768	1.930E-2	3.09E-3	1.562E-1	1.361E-1
12	.7795	2.859E-2	3.22E-3	1.562E-1	1.474E-1

3. CONCLUSION

The combined generators of the forms (3) and (2) are respectively equivalent and approximately equivalent to a LCG. This structural property might appear deceptive at first, because one of the goals of combination was to get rid of the lattice structure of the components. But in fact, they give a stronger theoretical basis to these combination approaches. They show that combination can be viewed as an efficient way of implementing (sometimes with added noise) a LCG with much larger modulus than the largest integer representable on the target computer. If well chosen, that LCG will have much better properties than any of its components. Selecting a combined generator should be based on the properties of its associated LCG rather than on those of its components. After extensive numerical investigations, we found that the quality (in terms of lattice structure) of the associated LCG is essentially unrelated to the quality of its individual components. This means that when searching for good combined generators, searching for individual components with the best lattice structure (as was done in [5]) is essentially useless. When the individual moduli differ enough (with $\delta_i = \pm 1$), the lattice structure of (7) is usually not recognizable by looking at the points produced by (2) in small dimensions. With appropriate parameters, combination (2) can be used to get rid of the lattice structure up to a given dimension.

An alternative approach, which yields a lattice structure of comparable quality to combination (3) and longer period, is to use a multiple recursive generator of order J (see [6, 7]).

ACKNOWLEDGMENTS

This work has been supported by NSERC-Canada grant # A5463 and FCAR-Québec grant # EQ2831. Raymond Couture, Marco Jacques, and François Paradis gave suggestions and helped computing the values for the numerical examples.

REFERENCES

[1] L. Afflerbach and H. Grothe, Calculation of Minkowski-Reduced Lattice Bases, *Computing*, **35** (1985), 269–276.

[2] U. Dieter, How to Calculate Shortest Vectors in a Lattice, *Math. of Computation*, **29**, 131 (1975), 827–833.

[3] H. Grothe, *Matrixgeneratoren zur Erzeugung gleichverteilter Pseudozufallsvektoren* (in german), Dissertation (thesis), Tech. Hochschule Darmstadt, Germany, 1988.

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

[5] P. L'Ecuyer, Efficient and Portable Combined Random Number Generators, *Communications of the ACM*, **31**, 6 (1988), 742–749 and 774. See also the correspondence in the same journal, **32**, 8 (1989), 1019–1024.

[6] P. L'Ecuyer, Random Numbers for Simulation, *Communications of the ACM*, **33**, 10 (1990), to appear.

[7] P. L'Ecuyer and F. Blouin, Multiple Recursive and Matrix Linear Congruential Generators, submitted for publication, 1990.

[8] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, 1986.

[9] S. Tezuka, *Analysis of L'Ecuyer's Combined Random Number Generator*, Technical report RT-5014, IBM Research, Tokyo Research Laboratory, 1989.

[10] S. Tezuka and P. L'Ecuyer, *Efficient and Portable Combined Tausworthe Random Number Generators*, Submitted for publication, 1990.

[11] B. A. Wichmann and I. D. Hill, An Efficient and Portable Pseudo-random Number Generator. *Applied Statistics*, **31** (1982), 188–190. See also corrections and remarks in the same journal by Wichmann and Hill **33** (1984), 123; McLeod **34** (1985), 198–200.

[12] H. Zeisel, A Remark on Algorithm AS 183, *Applied Statistics*, **35** (1986), 89.