MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 206
APRIL 1994, PAGES 799–808

ON THE LATTICE STRUCTURE OF CERTAIN LINEAR CONGRUENTIAL SEQUENCES RELATED TO AWC/SWB GENERATORS

RAYMOND COUTURE AND PIERRE L'ECUYER

ABSTRACT. We analyze the lattice structure of certain types of linear congruential generators (LCGs), which include close approximations to the add-with-carry and subtract-with-borrow (AWC/SWB) random number generators introduced by Marsaglia and Zaman, and also to combinations of the latter with ordinary LCGs. It follows from our results that all these generators have an unfavorable lattice structure in large dimensions.

1. INTRODUCTION

New classes of random number generators with astronomically long periods have been proposed and recommended recently for certain applications which may require billions of random numbers [5, 9, 10]. First, Marsaglia and Zaman [10] introduced the add-with-carry (AWC) and subtract-with-borrow (SWB) generators. Marsaglia, Narasimhan, and Zaman [9] then proposed a generator which combines a SWB with an LCG. Those generators looked promising at first sight, but statistical defects have quickly been discovered [2, 7]. The AWC/SWB generators have also been proved essentially equivalent to linear congruential generators (LCGs) with large moduli [11]. As a consequence, an AWC/SWB can be analyzed theoretically by examining the lattice structure of its associated LCG.

In general, to any LCG based on the recurrence

$$x_{i+1} \equiv a x_i + b \pmod{m}, \tag{1}$$

and for each dimension d, one may associate a lattice Λ_d in $\mathbf{R}^d$, generated by the vector $(1/m)(1, a, \ldots, a^{d-1})$ and $\mathbf{Z}^d$. It is well known [6] that the shorter vectors in the lattice $\Lambda^{(d)}$ dual to Λ_d afford critical information on the behavior of the generator. Algorithms to compute the shortest vector in a lattice are available [3]. However, the LCGs associated with the generators proposed in [10] have the peculiarity that their modulus can be fairly large (e.g.,

Received by the editor March 12, 1993.
1991 *Mathematics Subject Classification.* Primary 65C10.
Key words and phrases. Random number generation, lattice structure, combined generators.
This work has been supported by NSERC-Canada grant #OGP0110050 and FCAR-Québec grant #93ER1654 to the second author.

0025-5718/94 $1.00 + $.25 per page

$m \approx 10^{450}$), so that using directly the standard algorithms [3] to study $\Lambda^{(d)}$ and Λ_d can become impracticable in large dimensions.

In this paper, we study the smallest vectors in the lattices of certain classes of LCGs, which include the LCGs associated with the AWC/SWB generators. In the next section, we derive general results for the case where the modulus m can be expressed as a linear combination of powers of a, with small coefficients. We show how a set of short vectors in $\Lambda^{(d)}$ can be obtained a priori and, under certain conditions, extended into a basis for $\Lambda^{(d)}$. We then illustrate in §3 how these results can be used to analyze the LCGs associated with AWC/SWB generators. It follows, in particular, that all those LCGs have a bad lattice structure in large dimensions: for d larger than the largest lag of the AWC/SWB, the points in the d-dimensional unit hypercube lie in a set of parallel hyperplanes which are at least $1/\sqrt{3}$ apart. In §4, we examine a broader class of LCGs, for which m can be decomposed as $m = m_1 m_2$, where m_1 and m_2 are relatively prime, and m_1 is as in §2. Our results permit one to analyze, in particular, the (approximate) lattice structure of a class of generators which combine an AWC/SWB with an ordinary LCG. This is discussed in §§5 and 6. In one of our examples, we point out an important theoretical defect of the combined generator proposed by Marsaglia, Narasimhan, and Zaman [9]: in dimensions $d \geq 45$, the points lie in a set of parallel hyperplanes which are at least $1/\sqrt{6}$ apart. That could explain the statistical anomalies observed in [2]. We also point out general limitations of such combined generators.

We now recall some simple facts about lattices in Euclidean space. Given a lattice Λ in $\mathbf{R}^d$, the quantity $|\det(v_1, \ldots, v_d)|$ is independent of the choice of a basis $v_1, \ldots, v_d$ for Λ. We will call it the *volume* of Λ. The volume is inverted by passage from a lattice to its dual. If $\Lambda \subseteq \Lambda'$ are two lattices, then the (group-theoretical) index $[\Lambda' : \Lambda]$ (viewing Λ as a subgroup of Λ') is equal to the ratio of the volume of Λ to that of Λ'. As an illustration, since the index of $\mathbf{Z}^d$ in Λ_d is equal to m, we can infer that the volume of Λ_d is equal to $1/m$ and that of $\Lambda^{(d)}$ is equal to m.

2. Shortest vectors in a class of lattices

We will assume in this section that the modulus m is represented as $\sum_{i=1}^{n} c_i a^{i-1}$ for some integers $c_1, \ldots, c_n$, with $c_n \neq 0$. Although we do not make the requirement explicit, we are especially interested in the case of small coefficients c_i. The reader may also think of a as moderately sized while m could be rather large (see Example 1 below).

We denote by $e_1, \ldots, e_d$ the canonical basis in $\mathbf{R}^d$. It follows from the definition of $\Lambda^{(d)}$ that a vector $\sum_{i=1}^{d} z_i e_i$ belongs to it if and only if it has integral coordinates z_i satisfying the relation

$$\sum_{i=1}^{d} z_i a^{i-1} \equiv 0 \pmod{m}. \tag{2}$$

So, when the dimension satisfies $d \geq n$, the relation $m = \sum_{i=1}^{n} c_i a^{i-1}$ provides us with a vector $\sum_{i=1}^{n} c_i e_i$ in $\Lambda^{(d)}$ of magnitude comparable to that of the c_i's. We also note that we have a set of (moderately sized) vectors in $\Lambda^{(d)}$, namely the $w_i = ae_i - e_{i+1}$, $i = 1, \ldots, d-1$.

We first prove:

Proposition 1. *The lattice* $\Lambda^{(d)}$ *admits the basis formed by the set of vectors* $w_i = ae_i - e_{i+1}$, $i = 1, \dots, d-1$, *and* $w_d = \sum_{i<d} c_i e_i + (\sum_{i \geq d} c_i a^{i-d}) e_d$.

Proof. Let Λ (resp. Λ') be the subgroup of $\Lambda^{(d)}$ generated by the set $w_1, \dots, w_{d-1}$ (resp. $w_1, \dots, w_d$). We have $\Lambda \subseteq \Lambda' \subseteq \Lambda^{(d)}$. Now, since $w_d \equiv me_1 \pmod{\Lambda}$, the set $w_1, \dots, w_{d-1}, me_1$ is also a basis for Λ' whose volume is thus equal to $|\det(me_1, w_1, \dots, w_{d-1})| = m$. But this is also the volume of $\Lambda^{(d)}$, so $[\Lambda^{(d)} : \Lambda'] = 1$ and $\Lambda' = \Lambda^{(d)}$. □

We define a (linear) shift operator S over $\mathbf{R}^d$ by $Se_i = e_{i+1}$, for $i = 1, \dots, d-1$, and $Se_d = 0$. Clearly, S maps $\Lambda^{(d)} \cap (\mathbf{R}^{d-1} \times \{0\})$ into $\Lambda^{(d)}$.

Proposition 2. *Assume that* $d > n$, *so that* $w_d = \sum_{i=1}^{n} c_i e_i$. *Then, the set of vectors* $w_1, \dots, w_{n-1}, w_d, Sw_d, \dots, S^{d-n}w_d$ *generates a sublattice of* $\Lambda^{(d)}$ *of index equal to* $|c_n|^{d-n}$. *In particular, if* $|c_n| = 1$, *this set of vectors forms a basis for* $\Lambda^{(d)}$.

Proof. Let Λ' be this generated sublattice and let Λ be the lattice generated by the set $w_1, \dots, w_n$. We have $w_d \equiv me_1 \pmod{\Lambda}$ so that Λ' also admits the basis formed by the vectors $me_1, w_1, \dots, w_{n-1}, Sw_d, \dots, S^{d-n}w_d$. Its volume is thus equal to $m|c_n|^{d-n}$ and the index $[\Lambda^{(d)} : \Lambda']$ to $|c_n|^{d-n}$. □

Let H be the hyperplane in $\mathbf{R}^d$ generated by the set of vectors $w_1, \dots, w_{d-1}$. We view H as an Euclidean space with the metric inherited from that of $\mathbf{R}^d$. From Proposition 1 it follows that $H_\Lambda^{(d)} = \Lambda^{(d)} \cap H$ is the lattice in H generated by $w_1, \dots, w_{d-1}$.

Proposition 3. *The vectors* $w_1, \dots, w_{d-1}$ *are, with their opposites, the set of shortest vectors of* $H_\Lambda^{(d)}$.

Proof. We have

$$\begin{aligned}\|z_1 w_1 + \cdots + z_{d-1} w_{d-1}\|^2 \\ = a^2 z_1^2 + (z_1 - a z_2)^2 + \cdots + (z_{d-2} - a z_{d-1})^2 + z_{d-1}^2,\end{aligned}$$

and this cannot be smaller than $a^2 + 1$ if the z_i's are integral and not all zero. □

Let δ be the least distance to H for a point of $\Lambda^{(d)}$ not in H. In order to determine this distance we first find an expression for the volume of the lattice $H_\Lambda^{(d)}$. The square of that volume is equal to the determinant $|w_i \cdot w_j|_{i,j<d}$, which is equal to D_{d-1} if we define D_n (for each n) as the n-rowed determinant

$$D_n = \begin{vmatrix} a^2+1 & -a & 0 & \cdots \\ -a & a^2+1 & -a & \\ 0 & -a & a^2+1 & \\ \vdots & & & \ddots \end{vmatrix}.$$

Lemma 1. *For all positive integers n we have*

$$D_n = \frac{a^{2n+2} - 1}{a^2 - 1}.$$

Proof. Clearly $D_1 = a^2 + 1$ and, if we put $D_0 = 1$, we have the recurrence $D_n = (a^2 + 1)D_{n-1} - a^2 D_{n-2}$, $n \geq 2$, which can also be written as $D_n - D_{n-1} = a^2(D_{n-1} - D_{n-2})$. The results then follows by induction on n. □

Proposition 4. *One has*

$$\delta^2 = \frac{a^2 - 1}{a^{2d} - 1} m^2.$$

Proof. From a generalization of the formula giving the area of a parallelogram as the product of the height by the base, we see that δ is equal to the ratio of the volume of $\Lambda^{(d)}$ to that of $H_\Lambda^{(d)}$. The squares of those volumes are m^2 and D_{d-1}, respectively. The proposition then follows from Lemma 1. □

Theorem 1. *If the dimension d does not exceed $\frac{1}{2}\log_a(m^2 \frac{a^2-1}{a^2+1} + 1)$, then the vectors $w_1, \ldots, w_{d-1}$ are of shortest length in $\Lambda^{(d)}$.*

Proof. In view of Proposition 4, our hypothesis amounts to the inequality $a^2 + 1 \leq \delta^2$. The theorem then follows from Proposition 3. □

3. The AWC/SWB generators

As shown in [11], an AWC/SWB generator in base a, with lags $s < r$, can be closely approximated by an LCG (1) with multiplier a and modulus $m = a^r \pm a^s \pm 1$. According to Proposition 1, this representation of m gives us, for $d > r$, a vector of length $\sqrt{3}$ in $\Lambda^{(d)}$. As a result, all the points of Λ_d lie in equidistant parallel hyperplanes which are at least $1/\sqrt{3}$ apart. In other words, all AWC/SWB generators have a bad lattice structure in large dimensions. Proposition 2 tells us more: in any dimension $d > r + 1$, it gives us a system of $d - r$ vectors of length $\sqrt{3}$ which can be completed to a basis of $\Lambda^{(d)}$. This length is in fact minimal for all dimensions not exceeding the least integer f for which $a^f \equiv \pm 1 \pmod{m}$. After that, we have a smaller vector of length $\sqrt{2}$, namely $\pm e_1 - e_{f+1}$ (the sign being the same as in the congruence), and it is minimal for all succeeding dimensions. To show this, we remark that since $\Lambda^{(d)} \subset \mathbf{Z}^d$, vectors of length smaller than $\sqrt{3}$ are either of the form $\pm e_i$ or $\pm e_i \pm e_j$ $(i \neq j)$. Our statement then results from condition (2).

In dimensions $d < r$, according to Theorem 1, the lattice $\Lambda^{(d)}$ has $w_1, \ldots, w_{d-1}$ as a set of shortest vectors with their squared lengths equal to $a^2 + 1$. For $d = r$, one has $w_d = \pm e_1 \pm e_{s+1} + a e_d$, with squared length $a^2 + 2$, but the condition of Theorem 1 is no longer satisfied. Nevertheless, one can prove as follows that $a^2 + 1$ is again the squared length of a shortest vector in $\Lambda^{(d)}$. By Propositions 3 and 4, a vector of shorter squared length must be of the form (up to a sign) $z_1 w_1 + \cdots + z_{d-1} w_{d-1} + w_d$. Then, as in the proof of Proposition 3, it is easily seen, using the special form of w_d, that the squared length of such a vector must exceed a^2 if the coefficients z_i are all integral.

Example 1. One SWB generator recommended in [5, 10] has an associated LCG with multiplier $a = 2^{32} - 5$ and modulus $m = a^{43} - a^{22} + 1$. So, the length

of the shortest vector in $\Lambda^{(d)}$ is $\sqrt{a^2+1} \approx 2^{32} - 5$ for $d \leq 43$, $\sqrt{3}$ when $43 < d \leq (m-1)/2$, and $\sqrt{2}$ for $d > (m-1)/2$.

4. Decomposable moduli

The pseudorandom sequence obtained by combining in various ways two or more LCGs is equivalent (or, in some cases, almost equivalent) to the sequence produced by an LCG whose modulus is the product of the individual moduli [8]. So, special consideration of LCGs with decomposable moduli could be useful for studying such combinations. Combining an AWC/SWB generator with an LCG is not exactly the same as combining two LCGs, but almost, because of the "approximation" property proved in [11]. The results developed in this section will permit us to analyze the lattice structure of such combined generators.

When the modulus m admits a divisor m_1, the LCG sequence (1) also satisfies the same recurrence with m_1 as the modulus. The corresponding lattice $\Lambda_{1,d}$ is then contained in Λ_d. If m_2 is the complementary factor and $\Lambda_{2,d}$ is the corresponding lattice, then $\Lambda_d = \Lambda_{1,d} + \Lambda_{2,d}$, $\Lambda^{(d)} = \Lambda_1^{(d)} \cap \Lambda_2^{(d)}$, and the sum is direct modulo $\mathbf{Z}^d$ if m_1 and m_2 have no common factors. In such a case, the volume of Λ_d is equal to the product of the volume of $\Lambda_{1,d}$ with that of $\Lambda_{2,d}$ and the index $[\Lambda_1^{(d)} : \Lambda^{(d)}]$ is thus equal to m_2, the volume of $\Lambda_2^{(d)}$. Now, if $\Lambda_1^{(d)}$ contains a vector w whose last coordinate is equal to zero, then $\Lambda^{(d)}$ will contain the vector $a_2 w - Sw$, where a_2 is any integer satisfying the congruence $a_2 \equiv a \pmod{m_2}$. If w and the multiplier a_2 are small, this will provide us with a small vector in $\Lambda^{(d)}$. Generalizing this construction, we obtain:

Theorem 2. *Let $w \in \Lambda_1^{(d)}$ have its last l coordinates equal to zero $(0 < l < d)$. Take any $\sum_{i=1}^{l+1} z_i e_i \in \Lambda_2^{(l+1)}$. Then, the vector $\sum_{i=1}^{l+1} z_i S^{i-1} w$ belongs to $\Lambda^{(d)}$.*

Proof. Since the latter vector clearly belongs to $\Lambda_1^{(d)}$, we only need to prove that it belongs to $\Lambda_2^{(d)}$. For this, it is sufficient to show that $\sum_{i=1}^{l+1} z_i S^{i-1} e_j \in \Lambda_2^{(d)}$ for $j \leq d - l$. By hypothesis, $\sum_{i=1}^{l+1} z_i e_i \in \Lambda_2^{(l+1)}$, so that $\sum_{i=1}^{l+1} z_i a_2^{i-1} \equiv 0 \pmod{m_2}$ and therefore $\sum_{i=1}^{l+1} z_i a_2^{i+j-2} \equiv 0 \pmod{m_2}$ for $j \geq 1$. This implies that the vector $\sum_{i=1}^{l+1} z_i S^{i-1} e_j = \sum_{i=1}^{l+1} z_i e_{i+j-1}$ belongs to $\Lambda_2^{(d)}$. □

We note that the length of the vector $\sum_{i=1}^{l+1} z_i S^{i-1} w$ is bounded by $\|w\| \sum_{i=1}^{l+1} |z_i|$ and, in case the $S^i w$ are orthogonal, its squared length is equal to $\|w\|^2 \sum_{i=1}^{l+1} |z_i|^2$. It turns out that in many instances (see the examples in the next section) this construction gives a shortest vector in $\Lambda^{(d)}$.

We now assume for the rest of this section that m_1 and m_2 are relatively prime and that m_1 is represented as $\sum_{i=1}^{n} c_i a_1^{i-1}$ for some integers $c_1, \ldots, c_n$, with $c_n \neq 0$, and where a_1 is an integer satisfying the congruence $a_1 \equiv a \pmod{m_1}$. We will exhibit, in this situation, a basis of moderately sized vectors for the lattice $\Lambda^{(d)}$. We denote by a_2 any integer such that $a_2 \equiv a \pmod{m_2}$ and by $w_1^{(1)}, \ldots, w_d^{(1)}$ the basis for $\Lambda_1^{(d)}$ obtained from Proposition 1. We put

$$h_1 = a_1 - a_2, \qquad h_2 = \sum_{i<d} c_i a_2^{i-1} + a_2^{d-1} \sum_{i \geq d} c_i a_1^{i-d},$$

and we take $K = (k_{ij})$ any integral 2×2 matrix of determinant equal to m_2 and satisfying the system of congruences

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{m_2}. \tag{3}$$

(Such a matrix K always exists, for arbitrary integers h_1 and h_2.)

Proposition 5. *The lattice $\Lambda^{(d)}$ admits the basis formed by the set of vectors $a_2 w_i^{(1)} - S w_i^{(1)}$, $i = 1, \ldots, d-2$, and $k_{i1} w_1^{(1)} + k_{i2} w_d^{(1)}$ for $i = 1, 2$.*

Proof. Let Λ be the lattice generated by this set of vectors. From (3), the scalar product of each of the two vectors $k_{i1} w_1^{(1)} + k_{i2} w_d^{(1)}$ with the vector $(1, a_2, \ldots, a_2^{d-1})$ is congruent to 0 modulo m_2 and therefore, these two vectors belong to $\Lambda_2^{(d)}$. Since they also clearly belong to $\Lambda_1^{(d)}$, they are in the intersection $\Lambda^{(d)}$. The lattice Λ is thus contained in $\Lambda^{(d)}$. But since both indices $[\Lambda_1^{(d)} : \Lambda]$ and $[\Lambda_1^{(d)} : \Lambda^{(d)}]$ are equal to m_2, we must have $\Lambda = \Lambda^{(d)}$. □

Proposition 6. *Let $d > n$. Then the set of vectors $a_2 w_i^{(1)} - S w_i^{(1)}$ for $i = 1, \ldots, n-2$, $k_{i1} w_1^{(1)} + k_{i2} w_d^{(1)}$ for $i = 1, 2$, and $a_2 S^i w_d^{(1)} - S^{i+1} w_d^{(1)}$ for $i = 0, \ldots, d-n-1$, generates a sublattice of index $|c_n|^{d-n}$ in $\Lambda^{(d)}$. In particular, if $|c_n| = 1$, this set of vectors is a basis for $\Lambda^{(d)}$.*

Proof. Let Λ be the lattice generated by those vectors. As in the proof of the previous proposition, we see that Λ is a sublattice of $\Lambda^{(d)}$. Let Λ' be the lattice generated by the set of vectors $w_1^{(1)}, \ldots, w_{n-1}^{(1)}, w_d^{(1)}, S w_d^{(1)}, \ldots, S^{d-n} w_d^{(1)}$. Then, the index $[\Lambda' : \Lambda] = m_2$, so that $[\Lambda_1^{(d)} : \Lambda] = m_2 |c_n|^{d-n}$ by Proposition 2, and we finally obtain $[\Lambda^{(d)} : \Lambda] = [\Lambda_1^{(d)} : \Lambda] / [\Lambda_1^{(d)} : \Lambda^{(d)}] = |c_n|^{d-n}$. □

5. Numerical examples

We will now give numerical illustrations of the results of the previous section. We use the same notation as in the preceding section. For a_1 and m_1 we take the same values as in Example 1, so in each case we will specify values only for a_2 and m_2. Each example considered is closely related to the combination of the SWB of Example 1 with an LCG (that will be discussed in the next section). We denote by $w_{\min}$ a shortest vector in $\Lambda^{(d)}$. Our procedure for determining a shortest vector $w_{\min}$ is to use the lattice basis from Proposition 5 (or 6 if $d > 44$) as an input for the standard search algorithms [3]. We notice that, when $d > 44$, the vector obtained by Theorem 2 using $w = w_d^{(1)}$ with the shortest vector of $\Lambda_2^{(l+1)}$ ($l = d - 44$) happens to produce a $w_{\min}$ in all the cases we examined. A similar phenomenon occurs for $2 < d < 44$, but now using $w = w_1^{(1)}$ and taking $l = d - 2$.

Example 2. Let $a_2 = 1$ and $m_2 = 2^{32}$. Table 1 describes a shortest vector $w_{\min}$ for dimensions up to 46. For the intermediate dimensions 5 to 43 the result is identical to the dimension-4 entry. This example is closely related to the combined generator proposed in [9] (see next section).

Example 3. This example has $a_2 = 2736464641$ and $m_2 = 2^{32} - 23^2$. The modulus has the prime factorization $m_2 = 3 \times 7^3 \times 13 \times 41^2 \times 191$, and we

TABLE 1. A shortest vector for Example 2

d	$w_{\min}$	$\|w_{\min}\|$
2	$2^{31} w_1^{(1)}$	.92E19
3	$(1-S) w_1^{(1)}$	.61E10
4	$(1-S^2) w_1^{(1)}$	.61E10
⋮	⋮	⋮
43	$(1-S^2) w_1^{(1)}$	.61E10
44	$w_{23}^{(1)} + 6 w_d^{(1)}$	.43E10
45	$(1-S) w_d^{(1)}$	$\sqrt{6}$
46	$(1-S) w_d^{(1)}$	$\sqrt{6}$

TABLE 2. A shortest vector for Example 3

d	$w_{\min}$	$\|w_{\min}\|$
2	$(2^{32} - 23^2) w_1^{(1)}$	.18E20
3	$2009 (1-S) w_1^{(1)}$	.12E14
4	$7 (1-S)^2 w_1^{(1)}$	.74E11
5	$(1-S)^3 w_1^{(1)}$	.19E11
6	$(1 - 2S + 2S^3 - S^4) w_1^{(1)}$	.14E11
7	$(1 - 2S + 2S^3 - S^4) w_1^{(1)}$	.14E11
8	$(1 - S - S^2 + S^4 + S^5 - S^6) w_1^{(1)}$	.11E11
9	$(1 - S - S^2 + S^4 + S^5 - S^6) w_1^{(1)}$	.11E11
10	$(1-S)(1-S^7) w_1^{(1)}$	.86E10
11	$(1-S^2)(1-S^7) w_1^{(1)}$	.86E10
⋮	⋮	⋮
14	$(1-S^6)(1-S^7) w_1^{(1)}$	.74E10
⋮	⋮	⋮
44	$w_1^{(1)} - 3144796996 w_{44}^{(1)}$	.46E10
45	$41 \times 7^2 (1-S) w_{45}^{(1)}$	.49E4
46	$7(1-S)^2 w_{46}^{(1)}$	.30E2
47	$(1-S)^3 w_{47}^{(1)}$	$\sqrt{60}$
48	$(1 - 2S + 2S^3 - S^4) w_{48}^{(1)}$	$\sqrt{30}$
49	$(1 + S - S^3 - S^5) w_{49}^{(1)}$	$\sqrt{12}$
50	$(1 + S - S^3 - S^5) w_{50}^{(1)}$	$\sqrt{12}$

TABLE 3. A shortest vector for Example 4

d	$w_{\min}$	$\|w_{\min}\|$
44	$w_{23}^{(1)} + 1409018015\, w_{44}^{(1)}$	.35E10
45	$(40883 + 13915S)\, w_{45}^{(1)}$	.75E5
46	$(169 - 156S + 1225S^2)\, w_{46}^{(1)}$	.22E4
47	$(2 - S + 149S^2 - 163S^3)\, w_{47}^{(1)}$	.22E3
48	$(38 + 55S + 6S^2 - 18S^3 + 29S^4)\, w_{48}^{(1)}$	.75E2
49	$(9 + 8S + 5S^2 + 20S^3 + 22S^4 + 21S^5)\, w_{49}^{(1)}$	.39E2
50	$(14 - 7S + 2S^2 - 7S^3 + 3S^4 + 2S^5 + 4S^6)\, w_{50}^{(1)}$	.18E2
51	$(4 + 8S + 5S^2 - S^3 + 5S^4 - 2S^5 - 4S^6 - 8S^7)\, w_{51}^{(1)}$	.14E2
52	$(3 - S + 6S^2 + S^3 - S^4 + 6S^5 - S^7 - 2S^8)\, w_{52}^{(1)}$	$\sqrt{89}$

have $a_2 \equiv 1 \pmod{3 \times 13 \times 191}$, $a_2 \equiv 42 \pmod{41^2}$, and $a_2 \equiv 8 \pmod{7^3}$, insuring full period m_2 for any LCG based on the recurrence $x_{i+1} \equiv a_2 x_i + b_2 \pmod{m_2}$ with b_2 prime to m_2. A shortest vector is described in Table 2 for dimensions up to 50. Entries are identical for dimensions 11 to 13 and for dimensions 14 to 43.

Example 4. Here we will use $a_2 = 742938285$ with $m_2 = 2^{31} - 1$. This a_2 is one of the five best multipliers (in terms of the spectral test for dimensions 2 to 6) found by Fishman and Moore [4] for an MLCG with this modulus. A shortest vector is described in Table 3 for dimensions 44 to 52.

6. COMBINING AWC/SWB AND LCG GENERATORS

It follows from a theorem of Minkowski [1, p.184] that, for any given positive number V, there exist lattices in $\mathbf{R}^d$, of volume V and with a shortest vector $w_{\min}$, satisfying

$$\|w_{\min}\| \geq C_d \sqrt{d/(2\pi e)}\, V^{1/d}, \tag{4}$$

where $C_d = (d/(8\pi e))^{1/2d}$ is close to 1 as d increases. Now consider again, as in §3, an LCG with multiplier a and modulus $m = a^r \pm a^s \pm 1$. The associated lattice $\Lambda^{(d)}$ has volume equal to m, and there exist lattices in $\mathbf{R}^d$ of volume m and with a shortest vector of length greater than $\sqrt{d/(2\pi e)}\, m^{1/d}$ (approximately). This lower bound is, when $d = r + 1$ say, far in excess of $\sqrt{3}$, the length of the shortest vector for $\Lambda^{(d)}$ (it is approximately .42E10 for $d = 44$ in case of Example 1). In this sense the lattice $\Lambda^{(d)}$ is far from optimal and the corresponding AWC/SWB generator also shares this relative defect. In this section we investigate to what extent it is possible to improve an AWC/SWB generator by means of a suitable combination with an LCG.

A convenient recipe for combining an AWC/SWB with an LCG runs as follows. We consider an AWC/SWB with lags $s < r$ and base a_1. Let y_i, $0 \leq y_i < a_1$, be its integer output. Let $x_i^{(2)}$, $0 \leq x_i^{(2)} < m_2$, be an integer sequence satisfying $x_{i+1}^{(2)} \equiv a_2 x_i^{(2)} + b_2 \pmod{m_2}$. This will be the LCG

component. Let m^* be a positive integer. The three integers a_1, m_2 and m^* should be close to one another. The combination is then defined as the least positive residue of $y_i + x_i^{(2)}$ modulo m^*, normalized through division by m^*. (For simplicity, we limit ourselves to this case although it may in fact be useful to consider more general linear combinations with several LCG components. Our method extends to the more general situation with obvious modifications.)

Such a combination can be approximated by an LCG of the type discussed in §4, with $m_1 = a_1^r \pm a_1^s \pm 1$, and a_1, a_2, m_2 as above. We will refer to it as the LCG *associated* with the combination. We consider first the question of the size of the error ϵ_i in this approximation. Let $x_i^{(1)}$, $0 < x_i^{(1)} < m_1$, be an integer sequence satisfying $x_{i+1}^{(1)} \equiv a_1 x_i^{(1)} \pmod{m_1}$. Then $x_i = m_2 x_i^{(1)} + m_1 x_i^{(2)}$ will satisfy (1) with $m = m_1 m_2$, $b = m_1 b_2$, and a any solution of the pair of congruences $a \equiv a_1 \pmod{m_1}$ and $a \equiv a_2 \pmod{m_2}$. The uniform variates associated with the x- and y-sequences are respectively $x_i/m = x_i^{(1)}/m_1 + x_i^{(2)}/m_2$ and y_i/a_2. The error (modulo 1) ϵ_i is then determined by the conditions $\epsilon_i \equiv (y_i + x_i^{(2)})/m^* - x_i/m \pmod 1$ and $-1/2 < \epsilon_i \leq 1/2$. We have

Proposition 7. *If the sequences $x^{(1)}$ and y are properly synchronized, then*

$$|\epsilon_i| \leq 1/a_1 + (|a_1 - m^*| + |m_2 - m^*|)/m^*.$$

Proof. We have $|\epsilon_i| \leq |x_i^{(1)}/m_1 - y_i/a_1| + y|1/a_1 - 1/m^*| + x_i^{(2)}|1/m_2 - 1/m^*|$. The first difference on the right-hand side is bounded by $1/a_1$ according to [11], if the $x^{(1)}$- and y-sequences are correctly synchronized. The proposition then follows easily. □

We illustrate this with the combination proposed by Marsaglia, Narasimhan, and Zaman [9]. Its first component is the SWB with base $a_1 = 2^{32} - 5$ and lags $r = 43$, $s = 22$ so that $m_1 = a_1^{43} - a_1^{22} + 1$. Its second component is an LCG based on the recurrence $x_{i+1} \equiv x_i + 362436069 \pmod{2^{32}}$. The combination is defined using $m^* = 2^{32}$. According to the proposition, the associated LCG approximates the combination with an error bounded by $1/(2^{32} - 5) + 5/2^{32} \approx 6/2^{32}$. It follows that this combination has an approximate lattice structure. This particular lattice was studied in Example 2. Its dual lattice $\Lambda^{(d)}$ has a vector of length $\sqrt{6}$ in all dimensions $d \geq 45$.

A substantial improvement is obtained if we use for the second component the Fishman and Moore "optimal" LCG described in Example 4. We then have, in dimension 45 for example, a shortest vector of length 74801 (approximately) instead of the $\sqrt{6}$. This is however essentially the best that can be done with a second component having a modulus of that size, and is still far from the .42E10 given by (4) with $V = m_1 m_2$. In fact, if we denote by γ_d the upper bound on the length of the shortest vector for all lattices of volume 1 in $\mathbf{R}^d$, we have the following estimate.

Proposition 8. *The* LCG *associated with a combination of an* AWC/SWB *(with lags $s < r$) with an* LCG *(with modulus m_2) has in its dual lattice $\Lambda^{(d)}$ a vector of length not exceeding $\sqrt{3}\,\gamma_{d-r}\, m_2^{1/(d-r)}$ (resp. $\sqrt{3(d-r)}\,\gamma_{d-r}\, m_2^{1/(d-r)}$) when $r + 1 < d < \min(r + s - 1,\ 2r - s + 1)$ (resp. $d > r + 1$).*

Proof. We use the vector $\sum_{i=1}^{l+1} z_i S^{i-1} w$ with $l = d - r - 1$, $w = w_d^{(1)}$, and where the coefficients z_i are chosen so that $\sum_{i=1}^{l+1} z_i e_i$ is a shortest vector in $\Lambda_2^{(l+1)}$. It then follows from Theorem 2 that the former vector belongs to $\Lambda^{(d)}$, and we obtain easily the estimates for its length with the help of the remarks following the theorem. □

The constants γ_i are (well known and) smaller than $\sqrt{2}$ for $i \leq 8$ [1, p. 332]. Therefore, in all cases we are far from achieving (4) when $r + 1 < d \leq r + 8$.

Bibliography

1. J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, Berlin, 1959.
2. A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, *Monte Carlo simulations: hidden errors from "good" random number generators*, Phys. Rev. Lett. **69** (1992), 3382–3384.
3. U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471.
4. G. Fishman and L. Moore, *An exhaustive analysis of multiplicative congruential random number generators with modulus* $2^{31} - 1$, SIAM J. Sci. Statist. Comput. **7** (1986), 24–45.
5. F. James, *A review of pseudorandom number generators*, Comput. Phys. Comm. **60** (1990), 329-344.
6. D. E. Knuth, *The art of computer programming: Seminumerical algorithms*, vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.
7. P. L'Ecuyer, *Testing random number generators*, Proc. 1992 Winter Simulation Conference, IEEE Press, Piscataway, NJ, pp. 305–313.
8. P. L'Ecuyer and S. Tezuka, *Structural properties for two classes of combined random number generators*, Math. Comp. **57** (1991), 735–746.
9. G. Marsaglia, B. Narasimhan, and A. Zaman, *A random number generator for PC's*, Comput. Phys. Comm. **60** (1990), 345–349.
10. G. Marsaglia and A. Zaman, *A new class of random number generators*, Ann. Appl. Probab. **1** (1991), 462–480.
11. S. Tezuka, P. L'Ecuyer, and R. Couture, *On the lattice structure of the add-with-carry and subtract-with-borrow random number generators*, ACM Trans. Model. Comput. Sim. (to appear).

Département d'Informatique, Université Laval, Ste-Foy, Canada G1K 7P4
E-mail address: couture@ift.ulaval.ca

Département d'IRO, Université de Montréal, C.P. 6128, Succ. A, Montréal, Canada H3C 3J7
E-mail address: lecuyer@iro.umontreal.ca