MATHEMATICS OF COMPUTATION, VOLUME 25, NUMBER 114, APRIL, 1971

The Lattice Structure of Multiplicative Congruential Pseudo-Random Vectors*

By W. A. Beyer, R. B. Roof and Dorothy Williamson

Abstract. The lattice structure of points in an n-dimensional space produced by an appropriate grouping of pseudo-random numbers obtained from multiplicative congruential generators is discussed. Examples are given for $2 \leqq n \leqq 6$. The work is based on the theory of the reduction of positive quadratic forms in n variables.

1. Introduction. There have recently appeared several articles [3], [8], [13] discussing the distribution of points in an n-dimensional Euclidean space E^n obtained from multiplicative congruential pseudo-random generators. For example, if x_0, λ, β, μ, and n are given positive integers and if

$$x_i \equiv \lambda x_{i-1} \pmod{2^\beta} \qquad (i = 1, 2, \cdots) \tag{1}$$

or

$$x_i \equiv \lambda x_{i-1} + \mu \pmod{2^\beta} \qquad (i = 1, 2, \cdots), \tag{2}$$

Marsaglia [8] has shown that the points

$$(x_0, x_1, \cdots, x_{n-1}), (x_n, \cdots, x_{2n-1}), \cdots \tag{3}$$

may lie on relatively few hyperplanes in E^n. This idea goes back at least to Franklin [4], [5]. Wood [14] describes a method he used to show that the points actually form a simple lattice in the case $n = 2$. Because his methods and results may be of some interest, it was thought that a report giving further details would be appropriate. In addition, a procedure for an extension to $3 \leqq n \leqq 6$ is given. Examples are presented for $2 \leqq n \leqq 6$. A more complete discussion of the general theory is given.

The interest in the present work arises from the need to know whether the generator produces points (3) which lie on few hyperplanes or lie on many. In the first instance, the pseudo-random points will not be uniformly distributed through the hypercube and hence the generator is probably not "good."

While this discussion bears some similarity to that of Coveyou and MacPherson [3], it has some advantages. First, it exhibits precisely the structure of the sets defined by (3). Secondly, it avoids a discussion of the Fourier analysis of lattice structure in which Coveyou and MacPherson couch their work. On the other hand, the present analysis has not been extended beyond $n = 6$ (but it is possible to extend the analysis), while Coveyou and MacPherson discuss $2 \leqq n \leqq 10$.

Received June 5, 1970.

AMS 1969 *subject classifications.* Primary 6515, 1061, 1063.

Key words and phrases. Multiplicative congruential pseudo-random numbers, Lehmer pseudo-random numbers, Monte Carlo integration, random numbers, lattices of random points, testing of random numbers, reduced cells, positive quadratic forms, quadratic forms.

* Work performed under the auspices of the U. S. Atomic Energy Commission.

Copyright © 1971, American Mathematical Society

In Section 8 the relation between the discrepancy theory of Zaremba (and others) and the present theory is discussed.

Applications of pseudo-random numbers in Monte Carlo calculations are well known. Applications in digital communications, especially in space communications, may not be so well known. See [6].

The computations were done on the Maniac II computer of the Los Alamos Scientific Laboratory. The Madcap language was used for the coding. This language can readily process arbitrarily large integers which is a requirement of our computations.

2. A Lattice in E^n. A lattice G_n in E^n consists of all vectors of the form $\mathbf{y} = \mathbf{e}_0 + \sum_{i=1}^n \mathbf{e}_i y_i$ where the $\mathbf{e}_i$ ($1 \leqq i \leqq n$) are n fixed linearly independent vectors, the y_i are integers, positive, negative, or zero, and $\mathbf{e}_0$ is a fixed vector. (This definition is not standard in that the origin is not required to be in the lattice.) The $\{\mathbf{e}_i\}$ are said to form a basis of G_n. Put in other terms, a lattice G_n is a coset of a discrete subgroup H of the additive group of vectors in E^n where H has n linearly independent vectors. H is discrete if every $x \in H$ has a neighborhood free of points of H other than x. The basis vectors of G_n are then called generators of H.

Following van der Waerden [12, p. 276] one says the basis $\{\mathbf{e}_i\}$ is reduced (in the sense of Minkowski) if:

(1) $\mathbf{e}_1$ is the shortest (in the Euclidean norm) of all vectors $\sum_{i=1}^n \mathbf{e}_i y_i$ with the greatest common divisor of $y_1, y_2, \cdots, y_n$: $(y_1, \cdots, y_n)$, equal to 1,

(2) $\mathbf{e}_k$ is the shortest of all vectors $\sum_{i=1}^n \mathbf{e}_i y_i$ with $(y_k, \cdots, y_n) = 1$, for $k = 2, 3, \cdots, n$.

Let N_1 be the length of the shortest nonzero vector $\mathbf{S}_1 = \sum_{i=1}^n \mathbf{e}_i y_i$. Let N_2 be the length of the shortest vector $\mathbf{S}_2 = \sum_{i=1}^n \mathbf{e}_i y_i$ which is linearly independent of $\mathbf{S}_1$. And so on, one defines the successive minima $N_1, N_2, \cdots$. Then if the $\{\mathbf{e}_i\}$ are reduced, it was shown by Mahler and Weyl [12] that

$$|\mathbf{e}_i| \leqq \delta_i N_i, \qquad i = 1, 2, \cdots, n,$$

where $\delta_1 = 1$, $\delta_k = \max(1, \frac{1}{4}\delta_1 + \frac{1}{4}\delta_2 + \cdots + \frac{1}{4}\delta_{k-1} + \frac{1}{4})$ for $k = 2, \cdots, n$ and that

$$|\mathbf{e}_i| = N_i, \qquad i = 1, 2, 3, 4,$$

where $|\mathbf{e}|$ denotes the Euclidean norm. It is this result which connects the reduced bases with the more intuitive idea of the "size" of the fundamental "cell" in the lattice and makes our theory a tool to study the distribution of pseudo-random points in the n-cube.

Minkowski [9] has stated the following for $n \leqq 6$. $(\mathbf{e}_i)_{1 \leq i \leq n}$ is reduced if for every subset of $(\mathbf{e}_i)_{1 \leq i \leq n}$, say $(\mathbf{e}_{i_j})_{1 \leq j \leq k}$, one has

$$|\mathbf{e}_{i_j}| \leqq \left| \sum_{l=1}^{k} (\pm) C_l \mathbf{e}_{i_l} \right|, \qquad j = 1, 2, \cdots, k,$$

for all combinations of ± signs and $(C_l)_{1 \leq l \leq k}$ ranging over the following values. If $k = 2, 3$, and 4, $C_l = 1$. For $k = 5$, one of the C_l takes the values 1 and 2 and the remainder take the value 1. For $k = 6$, one of the C_l takes the values 1, 2, 3, another C_l takes the values 1 and 2, and the remainder take the value 1. (The cases $k = 5$, 6 are stated [9] without proof.)

The analysis given in van der Waerden [12] can be used to obtain algorithms for $n > 6$, but would not be optimal algorithms as is so for $2 \leqq n \leqq 6$.

For a set of vectors in E^n: $(\mathrm{a}_i)_{1 \leqq i \leqq n}$, define det (a_i) to be the $n \times n$ determinant whose ith row consists of the components of the vector a_i. It is easy to show (see Cassels [2, p. 11, lines 7 to 13]) that for a given lattice G_n, a set $(\mathrm{a}_i)_{0 \leqq i \leqq n}$ in G_n defines a basis $(\mathrm{a}_i - \mathrm{a}_0)_{1 \leqq i \leqq n}$ of G_n if and only if $0 < |\det(\mathrm{a}_i - \mathrm{a}_0)| \leqq |\det(\mathrm{a}_i' - \mathrm{a}_0')|$ for any any other set $(\mathrm{a}_i')_{0 \leqq i \leqq n}$ in G_n such that $\det(\mathrm{a}_i' - \mathrm{a}_0') \neq 0$. Further (see Cassels [2, pp. 9 and 10]), two sets $(\mathrm{a}_i)_{0 \leqq i \leqq n}$ and $(\mathrm{a}_i')_{0 \leqq i \leqq n}$ in G_n both define a basis of G_n if and only if there exists an $n \times n$ matrix T with integer entries and with $\det T = \pm 1$ (unimodular matrix) so that $[\mathrm{a}_i' - \mathrm{a}_0'] = T[\mathrm{a}_i - \mathrm{a}_0]$, where $[\mathrm{a}_i - \mathrm{a}_0]$ is the $n \times n$ matrix whose ith row is the vector $\mathrm{a}_i - \mathrm{a}_0$.

A reduction algorithm is a procedure for obtaining from a basis of a lattice a reduced basis. Reduction algorithms are described and applied for $2 \leqq n \leqq 6$.

3. The Lattice Structure of Multiplicative Congruential Pseudo-Random Vectors.

In this section n is an arbitrary positive integer. The following Lemmas 1 and 2 will be needed. They are taken from the book of Jansson [7, p. 68].

LEMMA 1. (1) *When* $\lambda \equiv 3 \pmod 8$ *and* $x_0 \equiv 1$ *or* $3 \pmod 8$, *each sequence produced by* (1) *is some permutation of all the numbers* $8\nu + 1$ *and* $8\nu + 3$ ($\nu = 0, 1, \cdots, 2^{\beta-3} - 1$).

(2) *When* $\lambda \equiv 3 \pmod 8$ *and* $x_0 \equiv 5$ *or* $7 \pmod 8$, *each sequence produced by* (1) *is some permutation of all the numbers* $8\nu + 5$ *and* $8\nu + 7$ ($\nu = 0, 1, \cdots, 2^{\beta-3} - 1$).

(3) *When* $\lambda \equiv 5 \pmod 8$ *and* $x_0 \equiv 1 \pmod 4$, *each sequence produced by* (1) *is some permutation of all the numbers* $4\nu + 1$ ($\nu = 0, 1, \cdots, 2^{\beta-2} - 1$).

(4) *When* $\lambda \equiv 5 \pmod 8$ *and* $x_0 \equiv 3 \pmod 4$, *each sequence produced by* (1) *is some permutation of all the numbers* $4\nu + 3$ ($\nu = 0, 1, 2, \cdots, 2^{\beta-2} - 1$).

Remark. A method of determining exactly what permutation occurs is illustrated by the following discussion.

Consider the case $\lambda \equiv 5 \pmod 8$ and $x_0 = 1$. Denote the sequence generated by $\lambda = 5$ by

$$S_0 = \{x_i^{(0)};\ i = 0, 1, 2, \cdots, 2^{\beta-2} - 1\} \tag{4}$$

with $x_i^{(0)} \equiv 5^i \pmod{2^\beta}$. So every multiplier $\lambda \equiv 5 \pmod 8$ with $0 < \lambda < 2^\beta$ occurs among the *odd* members of S_0. Every $\lambda \equiv 5 \pmod 8$, $0 < \lambda < 2^\beta$, multiplier has a representation of the form $\lambda = x_{2n+1}^{(0)} \equiv 5^{2n+1} \pmod{2^\beta}$. Let S_n be the sequence generated with $\lambda = x_{2n+1}^{(0)}$: $S_n = \{x_i^{(n)};\ i = 0, 1, \cdots, 2^{\beta-2} - 1\}$. One has

$$x_i^{(n)} \equiv [x_{2n+1}^{(0)}]^i \pmod{2^\beta}\ [5^{2n+1}]^i = \pmod{2^\beta}$$

$$= 5^{(2n+1)i} \pmod{2^\beta} = x_{(2n+1)i}^{(0)};$$

i.e. when the multiplier $\lambda \equiv x_{2n+1}^{(0)}$ is used, the sequence obtained from $x_{i+1} \equiv \lambda x_i \pmod{2^\beta}$, $x_0 = 1$, consists of selecting every $(2n + 1)$th number from (4), beginning with the first.

LEMMA 2. *If, in* (2), $\lambda \equiv 1 \pmod 4$ *and* $\mu \equiv 1 \pmod 2$, *then* (2) *produces a permutation of the numbers* $0, 1, 2, \cdots, 2^\beta - 1$.

The following lemma is needed in the subsequent development.

LEMMA 3. *Let* $A \subset E^n$ *be a point set such that every point in* A *has integer co-*

ordinates and there are $n + 1$ vectors in A, say $\mathbf{e}_i$, $0 \leqq i \leqq n$, so that $\mathbf{e}_i - \mathbf{e}_0$, $1 \leqq i \leqq n$, are linearly independent. Suppose for any $\mathbf{a}_i \in A$, $0 \leqq i \leqq n$, and any set of integers k_i, $1 \leqq i \leqq n$, it is so that $\mathbf{a}_0 + \sum_{i=1}^{n} k_i(\mathbf{a}_i - \mathbf{a}_0) \in A$. Then A is a lattice.

Proof. Choose $\mathbf{e}_j$, $0 \leqq j \leqq n$, in A so that $|\det(\mathbf{e}_i - \mathbf{e}_0)| = D$ has the least positive value where $1 \leqq i \leqq n$. By the hypothesis, every $\mathbf{e}_0 + \sum_{i=1}^{n} k_i(\mathbf{e}_i - \mathbf{e}_0) \in A$ where the k_i are arbitrary integers. Let $\mathbf{a}$ be an arbitrary vector in A. Since $\{\mathbf{e}_i - \mathbf{e}_0; i = 1, 2, \cdots, n\}$ is a linearly independent set, there exist real γ_i such that $\mathbf{a} - \mathbf{e}_0 = \sum_{i=1}^{n} \gamma_i(\mathbf{e}_i - \mathbf{e}_0)$. Suppose γ_j is not an integer for some j, $1 \leqq j \leqq n$. Form

$$\left|\begin{vmatrix} \mathbf{e}_1 - \mathbf{e}_0 \\ \vdots \\ \mathbf{e}_{j-1} - \mathbf{e}_0 \\ \mathbf{a} - [\gamma_j](\mathbf{e}_j - \mathbf{e}_0) - \mathbf{e}_0 \\ \mathbf{e}_{j+1} - \mathbf{e}_0 \\ \vdots \\ \mathbf{e}_n - \mathbf{e}_0 \end{vmatrix}\right| = \left|\begin{vmatrix} \mathbf{e}_1 - \mathbf{e}_0 \\ \vdots \\ \mathbf{e}_{j-1} - \mathbf{e}_0 \\ \sum_{i=1}^{n} (\gamma_i - \delta_{ij}[\gamma_j])(\mathbf{e}_i - \mathbf{e}_0) \\ \mathbf{e}_{j+1} - \mathbf{e}_0 \\ \vdots \\ \mathbf{e}_n - \mathbf{e}_0 \end{vmatrix}\right|$$

$$= \left|\begin{vmatrix} \mathbf{e}_1 - \mathbf{e}_0 \\ \vdots \\ \mathbf{e}_{j-1} - \mathbf{e}_0 \\ (\gamma_j - [\gamma_j])(\mathbf{e}_j - \mathbf{e}_0) \\ \mathbf{e}_{j+1} - \mathbf{e}_0 \\ \vdots \\ \mathbf{e}_n - \mathbf{e}_0 \end{vmatrix}\right| = |\gamma_j - [\gamma_j]|\, D$$

where $[\gamma_j]$ denotes largest integer in γ_j. Since $0 < |\gamma_j - [\gamma_j]|\, D < D$, it is false that D is the minimum positive value of $|\det(\mathbf{e}_i - \mathbf{e}_0)|$ where $\mathbf{e}_i \in A$. Thus the γ_i are integers and therefore every $\mathbf{a} \in A$ has a representation $\mathbf{a} = \mathbf{e}_0 + \sum_{i=1}^{n} \gamma_i(\mathbf{e}_i - \mathbf{e}_0)$ where the γ_i are integers. This completes the proof of the lemma. For a more general lemma, see Cassels [2, p. 78].

In Lemmas 4 to 8 the points defined by (1) or (2) and (3) or (1) or (2) and

$$(5) \qquad (x_0, x_1, \cdots, x_{n-1}), (x_1, \cdots, x_n), (x_2, \cdots, x_{n+1}), \cdots$$

are discussed. We make the following convention: The point sets (3) and (5) are to be regarded as point sets G_n in E^n which are continued by periodicity throughout E^n; i.e., if $(t_1, t_2, \cdots, t_n) \in G_n$, then $(t_1 + h_1 2^\beta, t_2 + h_2 2^\beta, \cdots, t_n + h_n 2^\beta) \in G_n$ for all positive, zero, and negative integers h_i.

Remark. It might be objected that points generated by (1) and (5) or (2) and (5) would make a poor random-point generator, since such points would be highly correlated over a short run. However, the points defined by (1) and (3) or (2) and (3) are a reasonably sized subset for small n of those mentioned before and a discussion of the lattice structure of (5) gives information about the lattice structure of (3).

LEMMA 4. *If in* (1) $\lambda \equiv 5 \pmod 8$ *and* $x_0 \equiv 1 \pmod 4$, *then the point set* G_n *given by* (5) *forms a lattice in* E^n.

Proof. If $\mathbf{u}_i$, $1 \leqq i \leqq n$, are the unit coordinate vectors in E^n and $\mathbf{x} \in G_n$, the vectors $\mathbf{x}$, $\mathbf{x} + 2^\beta \mathbf{u}_i$ are $n + 1$ vectors in G_n for which $(\mathbf{x} + 2^\beta \mathbf{u}_i) - \mathbf{x}$ are linearly independent. Let $\mathbf{x}_{i_j}$, $0 \leqq j \leqq n$, be $n + 1$ points of G_n, not necessarily distinct. Let k_i, $1 \leqq i \leqq n$, be arbitrary integers. Recall that $\mathbf{x}_{i_j} = (x_{i_j}, x_{i_j+1}, \cdots, x_{i_j+n}) = (x_{i_j}, \lambda x_{i_j} + h_1 2^\beta, \lambda^2 x_{i_j} + h_2 2^\beta, \cdots, \lambda^{n-1} x_{i_j} + h_{n-1} 2^\beta)$ for some integers h_i where x_{i_j} is the i_jth number generated by (1). Form

$$\mathbf{x} = \mathbf{x}_{i_0} + \sum_{j=1}^{n} k_j(\mathbf{x}_{i_j} - \mathbf{x}_{i_0})$$

$$= \left\{x_{i_0} + \sum_{j=1}^{n} k_j(x_{i_j} - x_{i_0}), \lambda\left[x_{i_0} + \sum_{j=1}^{n} k_j(x_{i_j} - x_{i_0})\right] + h_1 2^\beta, \cdots, \right.$$

$$\left. \lambda^{n-1}\left[x_{i_0} + \sum_{j=1}^{n} k_i(x_{i_j} - x_{i_0})\right] + h_{n-1} 2^\beta\right\}$$

where h_i are again integers and the k_j are arbitrary integers. Since every x in the sequence generated by (1) under the hypothesis on λ and x_0 has the form $4\nu + 1$, $\nu = 0, 1, \cdots, 2^{\beta-2} - 1$ (Lemma 1, Part 3), $x_{i_0} + \sum_{j=1}^{n} k_j(x_{i_j} - x_{i_0})$ has the form $4\nu + 1$ for some integer ν. But every number of this form can be expressed as $4\nu + 1 = 4\nu_1 + 1 + h2^\beta$ with $0 \leqq \nu_1 \leqq 2^{\beta-2} - 1$ and h, ν_1 as integers. Thus $\mathbf{x} \in G_n$. Lemma 3 can now be applied to give the conclusion of the theorem.

In a similar way, Lemmas 5 to 8 can be proved, using Lemmas 1, 2, and 3.

LEMMA 5. *If, in* (1), $\lambda \equiv 5 \pmod 8$ *and* $x_0 \equiv 3 \pmod 4$, *then the point set* G_n *given by* (5) *forms a lattice in* E^n.

LEMMA 6. *In* (1), *let* $\lambda \equiv 3 \pmod 8$ *or* $\lambda \equiv 5 \pmod 8$ *and let* x_0 *be odd. Then the set* (x_{2n}, x_{2n+1}), $n = 0, 1, 2, \cdots$, *is a lattice in* E^2.

LEMMA 7. *In* (1), *let* $\lambda \equiv 3 \pmod 8$. *Let* G_n *be the set of points in* (5) *determined with* $x_0 \equiv 1$, *or* $3 \pmod 8$ *and* G_n' *be the same set, but with* $x_0 \equiv 5$ *or* $7 \pmod 8$. *Then* $G_n \cup G_n'$ *forms a lattice in* E^n.

LEMMA 8. *In* (2), *let* $\lambda \equiv 1 \pmod 4$ *and* $\mu \equiv 1 \pmod 2$. *Then the set of points in* (5) *form a lattice in* E^n *and the basis vectors of the lattice do not depend on* μ. *The sequence* (x_{2n}, x_{2n+1}), $n = 0, 1, 2, \cdots$, *forms a lattice in* E^2.

Remark 1. The points x_i (extended by our convention) defined by

$$x_i \equiv 3x_{i-1} \pmod{2^3}, \qquad x_0 = 1,$$

do not form a lattice on the line.

Remark 2. The structure of sequences generated by other generators, such as

1. $x_{n+1} \equiv \lambda x_n + \mu \pmod{p^\beta}$ (p an odd prime),
2. $x_{n+1} \equiv \lambda x_n \pmod{10^\beta}$,
3. $x_{n+1} \equiv a_0 x_n + a_1 x_{n-1} + \cdots + a_j x_{n-j} \pmod p$ (p a prime),
4. $x_{n+1} \equiv x_n + x_{n-1} \pmod{2^\beta}$,

is discussed in Jansson [7] and a theory analogous to that discussed here might be developable.

4. Reduction Algorithm in the Case $n = 2$. Let G_2 be a lattice with a basis $(\mathbf{e}_1, \mathbf{e}_2)$. Then, by the discussion in Section 2, if w is an integer, $(\mathbf{e}_1, \mathbf{e}_2 + w\mathbf{e}_1)$ is a basis of G_2 since

$$\begin{bmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 + w\mathbf{e}_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ w & 1 \end{bmatrix} \begin{bmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{bmatrix}$$

and the matrix $\left(\begin{smallmatrix} 1 & 0 \\ w & 1 \end{smallmatrix}\right)$ is unimodular. w is chosen to minimize $(\mathbf{e}_2 + w\mathbf{e}_1)^2$. Hence w must satisfy $(\mathbf{e}_2 + (w - 1)\mathbf{e}_1)^2 \geqq (\mathbf{e}_2 + w\mathbf{e}_1)^2 \leqq (\mathbf{e}_2 + (w + 1)\mathbf{e}_1)^2$ or

$$(6) \qquad -\frac{\mathbf{e}_1\mathbf{e}_2}{\mathbf{e}_1^2} - \frac{1}{2} \leqq w \leqq -\frac{\mathbf{e}_1 \cdot \mathbf{e}_2}{\mathbf{e}_1^2} + \frac{1}{2}.$$

In order to determine w uniquely, the right-hand inequality in (6) is replaced by $<$ to give

$$(7) \qquad -\frac{\mathbf{e}_1 \cdot \mathbf{e}_2}{\mathbf{e}_1^2} - \frac{1}{2} \leqq w < -\frac{\mathbf{e}_1 \cdot \mathbf{e}_2}{\mathbf{e}_1^2} + \frac{1}{2}.$$

Call the basis $(\mathbf{e}_1, \mathbf{e}_2 + w\mathbf{e}_1)$ thus determined $(\mathbf{e}_1, \mathbf{e}_2')$. Replace the basis $(\mathbf{e}_1, \mathbf{e}_2')$ by a new basis $(\mathbf{e}_1 + w'\mathbf{e}_2', \mathbf{e}_2')$ where w' is the unique integer determined by

$$(8) \qquad -\frac{\mathbf{e}_1 \cdot \mathbf{e}_2'}{\mathbf{e}_2'^2} - \frac{1}{2} \leqq w' < -\frac{\mathbf{e}_1 \cdot \mathbf{e}_2'}{\mathbf{e}_2'^2} + \frac{1}{2}.$$

The above procedure is then iterated until two successive minimizing integers of the form w and w' are zero. The resulting basis $(\bar{\mathbf{e}}_1, \bar{\mathbf{e}}_2)$ is reduced since, from (7), $\bar{\mathbf{e}}_1^2 \geqq 2\bar{\mathbf{e}}_1 \cdot \bar{\mathbf{e}}_2 \geqq -\bar{\mathbf{e}}_1^2$ and, from (8), $\bar{\mathbf{e}}_2^2 \geqq 2\bar{\mathbf{e}}_1 \cdot \bar{\mathbf{e}}_2 \geqq -\bar{\mathbf{e}}_2^2$ and therefore

$$\bar{\mathbf{e}}_1^2 \geqq 2\,|\bar{\mathbf{e}}_1 \cdot \bar{\mathbf{e}}_2'| \quad \text{and} \quad \bar{\mathbf{e}}_2^2 \geqq 2\,|\bar{\mathbf{e}}_1 \cdot \bar{\mathbf{e}}_2|$$

which implies that $\bar{\mathbf{e}}_1$ and $\bar{\mathbf{e}}_2$ are in length less than or equal to the length of the diagonals of the parallelograms which have $\bar{\mathbf{e}}_1, \bar{\mathbf{e}}_2$ as adjacent sides. The above algorithm must eventually terminate since for each pair of steps of the algorithm for which w and w' is not both zero, the vectors $(\mathbf{e}_1, \mathbf{e}_2)$ with integer coordinates are replaced by a pair of vectors $(\mathbf{e}_1', \mathbf{e}_2')$ with integer coordinates such that $|\mathbf{e}_1'| \leqq |\mathbf{e}_1|$ and $|\mathbf{e}_2'| \leqq |\mathbf{e}_2|$, with strict inequality in one of the cases.

5. Reduction Algorithm in the Case $3 \leqq n \leqq 6$. Assume $3 \leqq n \leqq 6$. Let $E = (\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n)$ be a set of basis vectors of a lattice G_n. Stage 1 of the reduction algorithm consists in successively replacing each pair of distinct vectors in E by a reduced pair, using the reduction algorithm for $n = 2$. This replacement defines a unimodular transformation from E to new set of vectors E' and hence E' is a basis of G_n. This operation is repeated until no further reduction by pairs is possible.

Stage 2 of the algorithm consists in examining for each k-tuple $(\mathbf{e}_{i_j})_{1 \leq j \leq k}$ the vectors $\sum_{l=1}^{k} (\pm) C_l \mathbf{e}_{i_l}$ where the values of C_l are described in Section 2. If it is found for some combination of $\pm$ signs and C_l's and for some $\mathbf{e}_{i_j}$ that

$$|\mathbf{e}_{i_j}| > \left| \sum_{l=1}^{k} (\pm) C_l \mathbf{e}_{i_l} \right|,$$

the vector $\mathbf{e}_{i_j}$ is replaced by the vector $\mathbf{e}_{i_j}' = \sum_{l=1}^{k} (\pm) C_l \mathbf{e}_{i_l}$ (the transformation from $E = (\mathbf{e}_i)_{1 \leqq i \leqq n}$ to $E' = (\mathbf{e}_1, \mathbf{e}_2 \cdots, \mathbf{e}_{i_j}', \cdots, \mathbf{e}_n)$ is unimodular). Stage 1 of the algorithm is repeated on E'. The algorithm must terminate after a finite number of steps, since if a basis is altered by an operation in stages 1 or 2, the alteration consists in replacing a vector with integer coordinates with a shorter vector having integer coordinates.

Remark. In the initial consideration of the problem of finding reduced bases for $n > 2$, the search technique suggested by Coveyou and MacPherson [3] was considered with some modifications suggested in van der Waerden [12]. Without preliminary reduction it was found in a typical example (of the type discussed in this paper) about 10^{19} vectors would have had to be examined to find the shortest nonzero vector. Techniques used in crystallography were also considered (see Azároff and Buerger [1] and Roof [10]). Tests showed that these techniques were unsatisfactory for our purposes, due to lack of precision and the amount of search required.

6. Finding Bases for Multiplicative Congruential Pseudo-Random Points. To apply the reduction algorithm to the determination of reduced bases for pseudo-random points of the form (3) or (5), it is necessary to find a basis of these points. The method of finding a basis is illustrated by an example.

Consider the example of the generator (1) with $\lambda \equiv 5 \pmod 8$ and $x_0 \equiv 1 \pmod 4$. To find a set of basis vectors for G_n defined by (5), choose a set of $n + 1$ vectors in G_n as follows:

$$\mathbf{r}_0 = (1, \lambda, \lambda^2, \cdots, \lambda^{n-1}),$$

$$\mathbf{r}_i = (4\alpha_i + 1, \lambda(4\alpha_i + 1) + h_i^1 2^\beta, \cdots, \lambda^{n-1}(4\alpha_i + 1) + h_i^{n-1} 2^\beta),$$

$$i = 1, 2, \cdots, n,$$

where $\alpha_i, h_i^k, i = 1, 2, \cdots, n, k = 1, 2, \cdots, n - 1$, are arbitrary integers. A calculation gives

$$\det(\mathbf{r}_i - \mathbf{r}_0) = 2^{2+(n-1)\beta} \begin{vmatrix} \alpha_1 & h_1^1 & \cdots & h_1^{n-1} \\ \alpha_2 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \alpha_n & h_n^1 & & h_n^{n-1} \end{vmatrix}$$

and $|\det(\mathbf{r}_i - \mathbf{r}_0)|$ has its minimum nonzero value when $\alpha_1 = h_2^1 = h_3^2 = \cdots = h_n^{n-1} = 1$, the other determinant entries being zero. Thus a set of basis vectors of G_n is given by (with these choices for α_i and h_i^j)

$$\mathbf{r}_1 - \mathbf{r}_0 = 4(1, \lambda, \lambda^2, \cdots, \lambda^{n-1}),$$

$$\mathbf{r}_i - \mathbf{r}_0 = (0, 0, \cdots, 2^\beta, 0, \cdots, 0), \qquad i = 2, 3, \cdots, n,$$

where 2^β appears in the ith place.

7. Examples. Tables 1 to 5 present a few examples. It is hoped that the captions are self-explanatory, except for "figure of merit" defined for a reduced basis $\{y_i;\ i = 1, 2, \cdots, n\}$ by

$$\text{figure of merit} = \frac{\min\limits_{1 \leqq i \leqq n} |y_i|}{\max\limits_{1 \leqq i \leqq n} |y_i|}.$$

TABLE 1

Reduced bases for lattices defined by (5) in n-dimensions for the traditional generator: $x_i \equiv 5^{15}x_{i-1} \pmod{2^{35}}$, $x_0 \equiv 1 \pmod 4$.

```
                        n = 2

     148728            177304
    -439772            399828

Figure of merit =   3,89-01
Cosine of angle: 3.99-02

                        n = 3

    1351376           3459216          9668432
  -12520052           2632220         -3330708
    7001788           31449484        -17029604

Figure of merit =   2,84-01
Cosines of angles:-2,92-01  -1,23-01   1,08-01

                        n = 4

   77710304          39043680         57634528        -27397792
  -62468112          75233072        -63711888          1670832
   90632932          16799700        -88091708         -4290828
   -8465924          13009868         25674588       -127412820

Figure of merit =   8,24-01
Cosines of angles:-4,48-01   2,00-01   3,41-01   8,02-02  -2,23-02  -1,36-01
```

```
                    n = 5

  25827680     237787616     107896928      52851936    -186499232
 192251352     157110264     -62209128      69997240     225757016
 200526964    -247943196      45409428      18094468    -221466188
  30054476     -48263716    -197075412     277932604     132652812
 -40032076      34520868    -449541420    -183833916     -56888844

Figure of merit =  6,66-01
Cosines of angles:-2,46-02 -5,19-02 -3,48-01 -3,14-01 -3,81-01  4,64-01
                  6,78-02 -1,06-01 -2,04-01  1,87-01

                    n = 6

-305139696     650889424     269544080     478429520     394774800     49237456
-106314720     -15850080    -224044768     538719904    -146950624     59535264
 428761576      -6351672      20150824     548909064     776354920   -961483448
 140595992    -318464968    -278002984     -35706632     598755480    453202872
-625061744     -31756464    -370532592    -341922864    -235736688   -452912048
-173820160    -715470080      98881280     286065408     285583104    129760000

Figure of merit =  4,33-01
Cosines of angles: 2,71-01  2,80-01 -9,67-02 -2,22-01 -1,54-01  8,54-02
                  -5,19-02 -4,54-02  2,43-01  5,34-02 -1,56-01  1,53-01
                  -3,71-01  5,29-01 -1,59-01
```

TABLE 2
Reduced bases for lattices defined by (5) in n-dimensions for a "bad" generator:
$x_i \equiv 5x_{i-1}$(mod 2^{35}), $x_0 \equiv 1$ (mod 4).

```
                        n = 2

          4            20
 -6607641992     1321528408

Figure of merit =  3,03-09
Cosine of angle: 1,40-09

                        n = 3

          4            20           100
 -6861391488       52779928     263899640
 -1319498400    -6597492000    1372278368

Figure of merit =  1,49-08
Cosines of angles:-5,98-09  4,57-09  1,92-01

                        n = 4

          4            20           100           500
 -6871525460        2111068      10555340      52776700
 -1372194024    -6860970120      54887768     274438840
  -263883468    -1319417340   -6597086700    1374304868

Figure of merit =  7,29-08
Cosines of angles: 1,00-09  5,12-09 -3,33-08  1,96-01  3,84-02  1,96-01
```

```
                  n = 5

           4           20          100          500         2500
 -6871930788        84428       422140      2110700     10553500
 -1374301716  -6871508580      2195468     10977340     54886700
   274438132   1372190660   6860953300    -54971868   -274859340
   -52776564   -263882820  -1319414100  -6597070500   1374385868

Figure of merit =  3,64-07
Cosines of angles:-2,69-07 -1,35-07  1,46-07 -4,29-08  1,96-01 -3,92-02
                   7,68-03 -2,00-01  3,92-02 -1,96-01

                  n = 6

           4           20          100          500         2500        12500
  6871946996        -3388       -16940       -84700      -423500     -2117500
  1374386020   6871930100       -87868      -439340     -2196700    -10983500
  -274860316  -1374301580  -6871507900      2198868     10994340     54971700
    54887620    274438100   1372190500   6860952500    -54975868   -274879340
   -10555312    -52776560   -263882800  -1319414000  -6597070000   1374388368

Figure of merit =  1,82-06
Cosines of angles:-9,56-07 -8,70-07 -5,29-08 -3,11-07 -1,53-07  1,96-01
                  -3,92-02  7,83-03 -1,54-03 -2,00-01  3,99-02 -7,83-03
                  -2,00-01  3,92-02 -1,96-01
```

TABLE 3

Reduced bases for lattices defined by (5) in n-dimensions for the "shift and add" generator: $x_i \equiv (2^{17} + 5)x_{i-1} \pmod{2^{35}}$, $x_0 \equiv 1 \pmod 4$.

```
                         n = 2

      262136            262104
     -262132            262204

Figure of merit =  1.00 00
Cosine of angle: 7.63-05

                         n = 3

      262140            786412           1310620
     -786416          -1834928           1311120
 -1183269268         473151516         -46491508

Figure of merit =  1.22-03
Cosines of angles: 1.87-02  4.94-04  4.55-04

                         n = 4

     -262140           -786412          -1310620          65544100
     1572844           5242780          13106700             -2500
   486529588        1164395268        -519287020          56986468
 -1356543000          59243400         146270632         -18378680

Figure of merit =  4.93-03
Cosines of angles:-2.27-01  1.18-03 -3.42-04  3.28-03  4.85-03 -3.58-01
```

```
                           n = 5

      786424         2883544         9174840        19659800       -32773000
   544986936      1356543000       -59243400      -146270632        18378680
   148109424       486791728      1165181680      -517976400        50432368
    -1310708        -4980676       -17039060       -45873700       -32760500
  1373057856        -4980672       -16514752       -40630720         6561600

Figure of merit =  2,68-02
Cosines of angles: 5,50-03  6.91-03  2.95-05 -1,85-03  3.71-01 -4,07-03
                   3,71-01 -4,47-03  1,08-01  1,91-03

                           n = 6

      524284         2097132         7864220        26213900        65533500          -12500
     -786424        -2883544        -9174840       -19659800        32773000       819225000
  1373844280        -2097128        -7339912       -20970920       -26211400       262159000
  -549443340     -1373057852         5504980        21757732        79952820       255584900
  -163313628      -543414092     -1351300220        72350100       146268132      -346071180
    39845500       148371564       487578140      1166492300      -524530500        -47874132

Figure of merit =  4,69-02
Cosines of angles: 2,65-02 -1,62-02  2,51-02 -3,40-03  3,79-03  1,86-01
                   1,75-01 -2,14-01 -7,46-02 -3,27-01 -1,46-01  1,43-02
                   3,31-01 -1,22-01 -3,46-01
```

TABLE 4

Reduced bases for lattices defined by (5) in n-dimensions for a generator with a "randomly selected" multiplier: $x_i \equiv \lambda x_{i-1} \pmod{2^{35}}$ where $\lambda = 273673163157 \equiv 5 \pmod 8$ and $x_0 \equiv 1 \pmod 4$.

```
                    n = 2

   -83306          -365532
   394836            82660

Figure of merit =  9.29-01
Cosine of angle:-4,17-01

                    n = 3

  19835632         24341936         19367792
  -3506608          9360528        -19970096
  -5256076          1684356          2441172

Figure of merit =  1,64-01
Cosines of angles:-2,77-01 -7.18-02 -1.08-01

                    n = 4

 -49630292         18153244        -91924660         -795844
  62445036         49622620          6559628         27132028
   3439528         99229896         62545000        -75321208
 -46465684         21525692        115895660        104324060

Figure of merit =  5.13-01
Cosines of angles:-3,15-01 -2.75-01 -4.55-01  2.97-01  1.17-01  5.92-02
```

```
                        n = 5

   246340616      99260584     -36306488     183849320       1591686
   -83006312     203312248    -206669352     -50576712      75042072
  -155976676      92658660     287776692     106194884     109603092
  -258676968      29735252      41382372     179924404     -30763844
  -150242428     287746004     205046372    -149567436     -20257324

Figure of merit, =  6,86-01
Cosines of angles;-1,90-02 -1,65-01 -2,06-01 -2,93-01 -2,12-01 -9,47-02
                   1,45-01  2,44-01  4,15-01  4,49-01

                        n = 6

  -169068752    -497660176     325706160     122489712     235542576    -122993680
   233248740    -491058252       1622980     200144148     127531172     495229812
   533124172    -178348996     535620332    -408262820     262620300    -155963012
    76404386     120770932     129014916     158588116    -693265564     411112756
  -164957284    -502716980     115444668    -628502420    -575046948      37297676
  -491058252       1622980     200144148     127531172     495229812     49841318

Figure of merit =  6,77-01
Cosines of angles: 3,77-01  3,21-01 -3,91-01  1,43-01  3,59-01  1,22-01
                   1,62-01  3,58-02  3,21-01 -2,84-01  1,74-01 -1,87-01
                   3,00-01 -1,73-01 -2,71-01
```

TABLE 5

Reduced bases for lattices defined by (5) in n-dimensions for the generator: $x_i \equiv (2^{13} + 5)x_{i-1} \pmod{2^{47}}$. Note the unusual structure for $n = 5$, two basis vectors being $(0, 2^{47}, 0, 0, 0)$ and $(0, 0, 2^{47}, 0, 0)$.

```
                     n = 2

           4           32788
-17169389564         2099220

Figure of merit =  1,91-06
Cosine of angle: 2,69-07

                     n = 3

           4           32788       268763236
-17169389820             788         6459236
    -2094596    -17169403412      -111412836

Figure of merit =  1,57-02
Cosines of angles: 3,76-04 -6,61-03  1,20-04

                     n = 4

-17169389820             788         6459236    52946357492
 34342969340     34342969324     34342838172    33267785228
    -6283272    -51503980584     34336218936    -2099009226
-34334590196     34340874044     17167828012    -1280214096

Figure of merit =  7,79-01
Cosines of angles: 3,09-01 -3,05-01 -2,99-02 -2,89-01  4,53-02 -2,62-01
```

```
                        n = 5

       40          327880     2687632360 2203052245492O 17995003093416
       -0 140737488355328             -0              -0             -0
       -0              -0 140737488355328             -0             -0
      220         1803340    14781977980 -1956961485326 28603772836124
      -12          -98364     -806289708 -6609156736476   867524790750 8

Figure of merit =  7.75-02
Cosines of angles: 1.15-08   9.45-05  8.48-02   3.39-02  0.0        5.20-08
                  -9.02-09   4.27-04 -7.39-05   9.99-01

                        n = 6

 360576037316   154522417364   -171400652 44   240373550260    1715 4506628  -121997525612
-154398829144  1030192704584   240298155368   -600857423096   583795318568    29562222 0744
-669578975812   223181126828  -17165201014 8   343356370124  -257601200132   -494712152084
-326224686276   -51474653140   274733277404   188861195340   -17153706628    128555125612
-188802537120   497975135968   515027225184  -446485826592  -669623336096   -140440121120
  85844862172   -17106552756   515075414396   -51478855828   240283843868   -718168788596

Figure of merit =  3.43-01
Cosines of angles:-1.07-01  -1.41-01  -4.35-01  -1.93-01   2.25-01  -1.55-01
                  -3.27-02   3.27-01   4.04-02   3.47-01   2.20-01   1.40-01
                   1.61-01   1.83-02   2.00-01
```

The figure of merit provides some measure (neglecting angle) of the departure of the reduced cell from "squareness." $x.xx - 0a$ means $x.xx \cdot 10^{-a}$. The angles refer to angles between the edges. Angles between higher-dimensional flats have not been calculated, but it might be useful to do so. Each row of the tables lists the components of a vector.

It is seen from these tables that multipliers of simple structure, such as 5 or $2^{17} + 5$ produce lattices of points which depart greatly from a uniform distribution throughout the cube. Multipliers of more complex structure, such as 5^{15} or the "randomly" selected multiplier 273673163157 produce better lattices. A typical time for the computation of a table on Maniac II was 20 minutes. The CDC 6600 is perhaps 8 times faster than Maniac II.

It is hoped that more examples with a more complete discussion can be presented in the future.

8. Connection Between Lattices of Pseudo-Random Points and the Theory of Discrepancy. Zaremba [15], Schmidt [11], and others (see references in [11] and [15]) have discussed the notion of the discrepancy $D(S)$ of a finite number of points S in the unit cube $I_n \subset E^n$. The quantity $D(S)$ can be used to estimate the error in the evaluation of a multidimensional integral. As an example, if $f(x, y)$ is of bounded variation in the sense of Hardy and Krause over $\bar{I}_2$ and $S = \langle x_0, \cdots, x_{N-1} \rangle$ is an arbitrary sequence of points in I_2, then

$$\left| \int_{I_2} f(\mathbf{x})\, d\mathbf{x} - N^{-1} \sum_{k=0}^{N-1} f(\mathbf{x}_k) \right| \leqq V^2(f)D(S) + V(f(x, 1))D(X) + V(f(1, y))D(Y),$$

where V and V^2 denote one- and two-dimensional variation and X and Y are projections of S on the x and y axis respectively. Roth (see [15]) has proved that, for E^n,

$$D(S) \geqq C_n N^{-1} (\log N)^{(n-1)/2}$$

for some constant C_n.

It seems to be a reasonable conjecture that if the figure of merit (see Section 7) of a lattice G_n is very small, then $D(G_n \cap I_n)$ is large. Conversely, if the figure of merit is near 1, $D(G_n \cap I_n)$ is small.

It should be remarked that the application of this lattice theory to much shorter segments of the full period of the generator sequence depends on the extent to which the lattice properties are reflected in the segments.

Acknowledgment. The authors thank Dr. W. W. Wood of this laboratory for valuable help and suggestions in the preparation of this paper.

Postscript. After completion of the above paper, the following important paper came to the authors' attention:

R. R. Coveyou, "Random number generation is too important to be left to chance," *Studies in Appl. Math.*, v. 3, 1970, pp. 70–111.

That paper has things in common with our paper. However, our paper was written independently and differs from the former in important details. It was thought best to not revise the present paper.

University of California
Los Alamos Scientific Laboratory
Los Alamos, New Mexico 87544

1. L. V. Azároff & M. J. Buerger, *The Powder Method in X-Ray Crystallography,* McGraw-Hill, New York, 1958.

2. J. W. S. Cassels, *An Introduction to the Geometry of Numbers,* Die Grundlehren der math. Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Band 99, Springer-Verlag, Berlin, 1959. MR **28** #1175.

3. R. R. Coveyou & R. D. MacPherson, "Fourier analysis of uniform random number generators," *J. Assoc. Comput. Mach.,* v. 14, 1967, pp. 100–119. MR **36** #4779.

→ J. N. Franklin, "Deterministic simulation of random processes," *Math. Comp.,* v. 17, 1963, pp. 28–59. MR **26** #7125.

→ J. N. Franklin, "Equidistribution of matrix-power residues modulo 1," *Math. Comp.,* v. 18, 1964, pp. 560–568.

6. S. W. Golomb, L. D. Baumert, M. F. Easterling, J. J. Stiffler & A. J. Viterbi, *Digital Communications with Space Applications,* Prentice-Hall, Englewood Cliffs, N. J., 1964.

7. B. Jansson, *Random Number Generators,* Almquist & Wiksell, Stockholm, 1966. MR **36** #7297.

→ G. Marsaglia, "Random numbers fall mainly in the planes," *Proc. Nat. Acad. Sci. U.S.A.,* v. 61, 1968, pp. 25–28. MR **38** #3998.

9. H. Minkowski, "Zur Theorie der positiven quadratischen Formen," *J. Reine Angew. Math.,* v. 101, 1887, pp. 196–202.

10. R. B. Roof, Jr., *A Theoretical Extension of the Reduced-Cell Concept in Crystallography,* Los Alamos Scientific Laboratory Report, LA-4038, 1969.

11. W. Schmidt, "Irregularities of distribution. IV," *Invent. Math.,* v. 7, 1969, pp. 55–82. MR **39** #6838.

→ B. L. van der Waerden, "Die Reduktionstheorie der positiven quadratischen Formen," *Acta Math.,* v. 96, 1956, pp. 265–309. MR **18,** 562.

13. P. H. Verdier, "Relations within sequences of congruential pseudo-random numbers," *J. Res. Nat. Bur. Standards Sect. B,* v. 73B, 1969, pp. 41–44. MR **39** #1081.

14. W. W. Wood, "Monte Carlo calculations for hard disks in the isothermal-isobaric ensemble," *J. Chem. Phys.,* v. 48, 1968, pp. 415–434.

15. S. K. Zaremba, "The mathematical basis of Monte Carlo and quasi-Monte Carlo methods," *SIAM Rev.,* v. 10, 1968, pp. 303–314. MR **38** #1810.