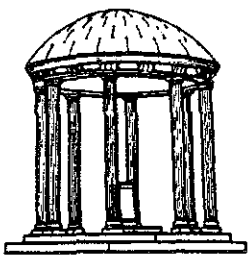
On a New Class of Independent Families of Linear Congruential Pseudo-Random Sequences

TR87-001

1987

John H. Halton



The University of North Carolina at Chapel Hill
Department of Computer Science
CB#3175, Sitterson Hall
Chapel Hill, NC 27599-3175

ON A NEW CLASS OF INDEPENDENT FAMILIES OF LINEAR CONGRUENTIAL PSEUDO-RANDOM SEQUENCES

JOHN H. HALTON

The University of North Carolina
Department of Computer Science
New West Hall 035A
Chapel Hill, NC 27514 USA

28 November 1986

ON A NEW CLASS OF INDEPENDENT FAMILIES OF LINEAR CONGRUENTIAL PSEUDO-RANDOM SEQUENCES

John H. Halton
Computer Science Department
University of North Carolina
Chapel Hill, NC 27514, USA

ABSTRACT

A class of families of linear congruential pseudo-random sequences is defined, for which it is possible to *branch* at any event without changing the sequence of random numbers used in the original random walk, and for which the sequences in different branches are statistically independent of each other. This is a hitherto unobtainable and computationally desirable tool.

1. INTRODUCTION

During the last forty or fifty years, the *Monte Carlo method* has been used with considerable success, to solve large mathematical problems too computationally complicated to yield to the classical numerical methods developed during the previous four centuries. For general discussions, the reader is referred to, e.g., BUS 62, HAM 64, HAL 70, ERM 71, SOB 73, KLE 75, YAK 77, or RUB 81. In particular, there is an extensive history of the effective application of the Monte Carlo method to *particle-transport problems*, such as arise in the design of radiation-shielding, nuclear reactors, and fission and fusion bombs (see, e.g., CAR 75, SPA 69).

While the method was originally conceived in terms of *representing the solution of a problem as a parameter of a hypothetical population, and using a* [truly] *random sequence of numbers to construct a sample of the population, from which statistical estimates of the parameter can be*

obtained (see HAL 70); it soon became apparent, from the point of view of the need both for repeatable results to debug Monte Carlo computer programs and for a large, stable supply of suitable 'random numbers', that certain deterministic sequences exhibiting some of the properties of truly random sequences were more useful in practice. These became known as *pseudo-random sequences* (and, by corruption, as sequences of 'pseudo-random numbers') (see the abovementioned references, and also LEH 51, HUL 62, TAU 65, JAN 66, and NIE 78). Somewhat later, even less random-looking sequences, dubbed *quasi-random*, having exceptionally good uniformity properties leading to fast convergence of the resulting Monte Carlo estimates, were proposed (see HAM 60, HAL 60, ZAR 66, and HAL 72). The uniformity of distribution of even the pseudo-random sequences was found to be imperfect (FRA 63, GRE 65, MAR 72), and a non-statistical approach was developed for error-analysis.

One of the most successful classes of pseudo-random number generators is the so-called *linear congruential* algorithm (originally due to Lehmer; see LEH 51): the sequence $[\xi_0, \xi_1, \xi_2, \xi_3, \ldots] = [\xi_j]_{j=0}^{\infty}$ of *canonical* [*pseudo-*]*random numbers*, which should be independently uniformly distributed in $[0, 1)$, is obtained from the integer sequence $[x_j]_{j=0}^{\infty}$ by

$$\xi_j = x_j/2^M, \tag{1}$$

where the x_j are uniquely determined by

$$(\forall j \geqslant 0)\ 0 \leqslant x_j < 2^M, \quad x_{j+1} \equiv ax_j + b \pmod{2^M}; \tag{2}$$

that is to say, given the parameters a and b and an intial integer x_0, each successive x_{j+1} is the *remainder* when $ax_j + b$ is divided by 2^M. In a binary computation, this is the integer consisting of the M least significant bits of $ax_j + b$.

Many calculations using the Monte Carlo method, including those of particle-transport alluded to above, involve the use of a long sequence of pseudo-random numbers to generate a sequential history of flights and collisions, usually referred-to as a *random walk*. By averaging so-called *scores*, which are functions of the random walk generated in this way, over large numbers of such random histories, it is possible to estimate the parameters of interest with considerable accuracy.

It is clear that two different sequences of random numbers will, in general, produce two different random-walk histories, and that these, in turn, will generally lead to different scores. While it is inherent in the Monte Carlo method that the results should show random fluctuations, it is extremely convenient to be able to reproduce a given result exactly, when we wish to do so. In particular, this is important in the initial, 'debugging' stage of developing a new program (or part of a program) to do correctly what the programmer intends; it is also useful when several runs must be made to develop intentionally correlated random variables, all depending on the same random walk; and finally, when it is attempted to refine the physics underlying a computation by taking into account some concomitant variables or even particles, it is useful to compare the scores obtained with and without the refinements, for the same random walks. While these aims can, in part, be achieved by storing the values of the thousands, or even millions, of random numbers required, it would be more convenient to adjust the random generator (algorithm) so as to be able to achieve these ends. The original invention of pseudo-random sequences was for this purpose, and the present development is a further move in this direction.

This problem was first raised by Warnock (see WAR 83) and suggestions of a general nature were made by him as to its solution. The author wishes to acknowledge several interesting discussions of the question with Dr Warnock. The present paper presents a possible explicit approach to the task of generating a large number of pseudo-random sequences which are mutually independent in a rigorously specified manner.

2. ANALYSIS OF LINEAR CONGRUENTIAL GENERATORS

We consider the sequence defined by (2). Here, it is assumed that a and b are themselves integers in $[0, 2^M)$. It is easily verified by induction that

$$x_n \equiv a^n x_0 + S_n(a)b \pmod{2^M}, \tag{3}$$

where $$S_n(a) = 1 + a + a^2 + a^3 + \ldots + a^{n-1}. \tag{4}$$

If $a = 1$, we have

$$S_n(1) = n \quad \text{and} \quad x_n \equiv x_0 + nb \pmod{2^M}; \tag{5}$$

If $a \geqslant 2$, we have

$$S_n(a) = (a^n - 1)/(a - 1). \tag{6}$$

It is clear that the generator (2) is *periodic*; for there are only 2^M possible values of all the x_j, and if some $x_i = x_j$, then thereafter all $x_{i+k} = x_{j+k}$ $(k = 1, 2, 3, \ldots)$; but the first $2^M + 1$ values in the sequence must necessarily have at least one such identity. If we choose i and j defined by the identity of x_i and x_j to be minimal, then it is evident that $p = j - i$ is the *period* of the sequence, with all x_0, x_1, x_2, ..., x_{i+p-1} different. If the period is maximal, with $p = 2^M$, then all possible integer values (modulo 2^M) occur in every period and, incidentally, $i = 0$, necessarily.

The generator (2) will have maximal period 2^M, therefore, if, by (3), 2^M is the least value of n such that

$$x_0 = x_n \equiv a^n x_0 + S_n(a)b \pmod{2^M}, \tag{7}$$

and, by (5) or (6), this is equivalent to

$$S_n(a)[(a - 1)x_0 + b] \equiv 0 \pmod{2^M}. \tag{8}$$

If a is *even*, there will certainly be a minimal t such that $a^t \equiv 0 \pmod{2^M}$; and then, for any $n \geqslant t$, by (3), $x_n \equiv S_n(a)b$, and, by (4), $S_n(a) = S_t(a) + a^t S_{n-t}(a) \equiv S_t(a)$; so that $x_n \equiv S_n(a)b \equiv S_t(a)b \equiv x_t \pmod{2^M}$. Since both x_t and x_n lie in $[0, 2^M)$, it follows that $x_n = x_t$; so that the period is 1, which is hardly maximal! Thus, a must be *odd*. We may then write

$$a = (2r - 1)2^q - 1, \tag{9}$$

where the positive integers q and r are clearly unique.

Now, by (4), $S_n(a)$ is the sum of n odd numbers, and will therefore be even only if n is even. Since $(a - 1)x_0$ is certainly even, the parity of the factor $[(a - 1)x_0 + b]$ is the same as that of b; if (8) holds, the product on the left of (8) must be divisible by 2^M, so that we tend to lengthen the period of (2) by making b *odd*; we now suppose that this is the case, and then we see that the period is maximal if $S_n(a)$ is divisible by 2^M only if $n = 2^M$.

We now observe that

$$\begin{aligned} S_{2m}(z) &= 1 + z + z^2 + z^3 + \ldots + z^{2m-2} + z^{2m-1} \\ &= (1 + z)(1 + z^2 + z^4 + \ldots + z^{2m-2}) \\ &= (1 + z)S_m(z^2). \end{aligned} \tag{10}$$

Given (9), we see that

$$1 + a = (2r - 1)2^q, \tag{11}$$

and $1 + a^{2m} = 1 + [(2r - 1)2^q - 1]^{2m} = 1 + [1 - (2r - 1)2^q]^{2m}$

$$= 2 - 2m(2r - 1)2^q + \Sigma_{h=2}^{2m} \binom{2m}{h} (2r - 1)^h 2^{hq} (-1)^{2m-h}, \qquad (12)$$

for any positive integer m. Every term on the right of (12) is clearly an integer; and every term except the 2 is divisible at least by 4; so that $1 + a^{2m}$ is divisible by 2 but *not* by 4. Thus, in order that $S_n(a)$ should be divisible by 2^M, it is necessary that n be divisible by 2^{M-q+1}; for then we can apply (10) repeatedly to yield that

$$S_n(a) = (2r - 1)2^q(1 + a^2)(1 + a^4)(1 + a^8)\ldots(1 + a^{2^{M-q}}) S_{n/2^{M-q+1}}(a), \qquad (13)$$

If the period is maximal, we need to have $n = 2^M$, or $q = 1$. Therefore the condition for maximal period is that

$$a \equiv 1 \pmod 4 \quad \text{and} \quad b \equiv 1 \pmod 2. \qquad (14)$$

Note that these conditions are satisfied by many choices of a and b, and are independent of the initial value x_0. Indeed, there are 2^{M-2} choices of a and 2^{M-1} choices of b. For every such choice, the period of length 2^M begins at once, with x_0 (i.e., $x_{2^M} = x_0$, and, thereafter, $x_{2^M+k} = x_k$, for $k = 1, 2, 3, \ldots$), and every possible integer value in $[0, 2^M)$ occurs just once (in a fixed order) in the period. There are 2^{2M-3} choices of parameters (not necessarily leading to different periodic orders), out of $(2M)!$ possible permutations of 2^M integers.

Let us write $2^u \parallel N$, for any non-negative integer u and integer N, to denote that 2^u, but not 2^{u+1}, divides N without remainder. As usual, we write $2^u \mid N$ when 2^u divides N, but 2^{u+1} might also divide N. Suppose now that b is *even*, and that, for some integer $c \geq 1$,

$$2^c \parallel b. \tag{15}$$

If we strengthen (14) (which was imposed to ensure that $q = 1$) to

$$a \equiv 5 \pmod 8, \tag{16}$$

then, by (9) with $q = 1$, $2(2r - 1) - 1 = 8s + 5$, for some integer s; whence $4r = 8(s + 1)$, or $a = 8(s + 1) - 3$, or $a - 1 = 8(s + 1) - 4$. In other words,

$$4 \parallel (a - 1). \tag{17}$$

[If $a \equiv 1 \pmod 8$, then, similarly, $2(2r - 1) - 1 = 8s + 1$; whence $4r = 8s + 4$, or $a = 8s + 1$, or $a - 1 = 8s$; so that $8 \mid (a - 1)$.] Now consider the factor

$$f(a, b, x_i) = (a - 1)x_i + b = f \tag{18}$$

from (8), generalized to any x_i. If, as we shall henceforth assume, (16) holds, and

$$2^t \parallel x_i, \tag{19}$$

then

$$\left.\begin{aligned} &t + 2 < c \Rightarrow 2^{t+2} \parallel f, \quad t + 2 > c \Rightarrow 2^c \parallel f, \\ \text{and} \quad &t + 2 = c \Rightarrow 2^{c+1} \mid f. \end{aligned}\right\} \tag{20}$$

By the same line of argument as was used above when b was odd, we see that the resulting sequence $x_0, x_1, x_2, \ldots$ has a period 2^{M-u}, where

$$2^u \parallel f. \tag{21}$$

[This follows from (8), (13), and (17), with u determined as in (20).] Further, by (2) with (19), if $t < c$, then $2^t \parallel x_j$ for every $j \geq i$; while, if $t > c$, then $2^c \parallel x_{i+1}$ and then $2^{c+1} \mid x_{i+2}$, and so on, so that, if $t \geq c$, alternate x_j are odd and even multiples of 2^c.

We may summarize our results as follows:

Theorem 1: *If the sequence* $[x_j]_{j=0}^{\infty}$ *is generated by* (2), *where* (15), (16), *and* (19) *hold, then the sequence will be periodic. The period will be given, for* c *defined as in* (15) *and* t *defined as in* (19), *by:*

(Case A) $c = 0$: *period* $= 2^M$;

(Case B) $c \geq 1$, *(i)* $t + 2 < c$: *period* $= 2^{M-t-2}$;

(ii) $t + 2 = c$: *period* $= 2^{M-u}$, *with* $u > c$;

(iii) $t + 1 = c$: *period* $= 2^{M-c}$;

(iv) $t \geq c$: *period* $= 2^{M-c}$.

Proof: ⟦We have shown that the period for odd b ($c = 0$, in (15)) is 2^M, yielding Case A; and that, for even b ($c \geq 1$), the period is 2^{M-u}, where u satisfies (21). By (20), in Case B(i), $u = t + 2$, in Case B(ii), $u > c$, and in Cases B(iii) and B(iv), $t + 2 > c$, so that $u = c$.⟧

Theorem 2: *In every case, with the same postulates as in Theorem 1, (a) the periods begin with* x_0, *and (b) the numbers occurring in each period are equally-spaced, modulo* 2^M.

⟦(a) Consider the sequence $1, a, a^2, a^3, \ldots$, reduced modulo 2^M. Since there are only 2^{M-1} distinct odd values in $[0, 2^M)$, it is clear that there must be $0 \leq i < 2^{M-1}$ and $0 < m \leq 2^{M-1}$ such that $a^i \equiv a^{i+m} \pmod{2^M}$. The difference $a^{i+m} - a^i$ must be divisible by 2^M and is clearly also divisible by a^i; since a is odd, it follows that $a^m - 1$ must also be divisible by 2^M, i.e., that $a^m \equiv 1 \pmod{2^M}$. If we find a period, as we have shown that we must, with $x_i \equiv x_{i+p} \pmod{2^M}$, then $a^{m-1}(x_i - b) \equiv a^{m-1}(x_{i+p} - b)$; and, by (2), $x_j - b \equiv ax_{j-1}$; so that $x_{i-1} \equiv a^m x_{i-1} = a^{m-1}ax_{i-1} \equiv a^{m-1}ax_{i+p-1} \equiv x_{i+p-1}$.

By induction, we see that eventually we must reach $x_0 \equiv x_p \pmod{2^M}$.

(b) We consider the various cases listed in Theorem 1. (A) $c = 0$: period 2^M. We have already shown that the interval $J_M = [0, 2^M)$ contains just 2^M integers, all of which therefore occur just once in the period. They are therefore equally-spaced, with spacing 1.

(B)(i) $t + 2 < c$: period 2^{M-t-2}. As in Cases (B)(ii) and (B)(iii), $t < c$, and we have seen that then every $x_j = K_j 2^t$, where K_j is odd. Indeed, by (2),

$$K_{j+1} \equiv aK_j + 2^{-t}b \pmod{2^{M-t}}, \tag{22}$$

where $2^{-t}b$ is an even integer, by (15). In the present case, since we must assume that

$$c \leqslant M, \tag{23}$$

and here $c \geqslant 3$, it follows that $M - t \geqslant c - t \geqslant 3$; whence, by (16) and (22), $K_{j+1} \equiv aK_j \equiv K_j \pmod 4$. Now, the number of integers K congruent to K_0 modulo 4 and lying in J_{M-t} is just 2^{M-t-2}; so all of these must occur just once in each period, and these values are equally-spaced, with spacing 2^{t+2}.

(B)(ii) $t + 2 = c$: period 2^{M-u}, where u is defined by (21). If we write

$$f_j = f(a, b, x_j) = (a - 1)x_j + b, \tag{24}$$

for a given sequence, following (18), then we see that, by Part (a) of the present theorem,

$$f_0 = F2^u, \tag{25}$$

where F is odd. Let

$$b = B2^c, \tag{26}$$

similarly, where B is also odd, by (15). By (17), we see that, if

$$a - 1 = 4A, \tag{27}$$

where A is odd, then we can write, by (24),

$$f_j = 2^c(AK_j + B). \tag{28}$$

Thus, by (22), we see that $f_{j+1} \equiv 2^c\{A[(4A + 1)K_j + 4B] + B\} \pmod{2^M}$,

which simplifies to $f_{j+1} \equiv 2^c(AK_j + B)(4A + 1)$

or $$f_{j+1} \equiv \alpha f_j. \tag{29}$$

Thus, $$f_j \equiv \alpha^j f_0 \pmod{2^M}; \tag{30}$$

and since, by (2) and (24),

$$f_j \equiv x_{j+1} - x_j \pmod{2^M}, \tag{31}$$

it follows that

$$x_j \equiv x_0 + S_j(\alpha) f_0 \pmod{2^M}. \tag{32}$$

Apart from an offset of x_0, the values of the x_j in any period take the values of $S_j(\alpha)f_0 = S_j(\alpha)F2^u$ reduced modulo 2^M, for $j = 0, 1, 2, \ldots, 2^{M-u} - 1$. No two of these numbers are the same; for, if, for instance, $S_i(\alpha)F2^u \equiv S_j(\alpha)F2^u \pmod{2^M}$, with $i < j$, then $[S_i(\alpha) - S_j(\alpha)]F2^u$ would be divisible by 2^M, or $S_i(\alpha) - S_j(\alpha) = \alpha^i S_{j-i}(\alpha)$ would be divisible by 2^{M-u}, and, since α is odd, this would require, by (13), that $j - i$ be itself divisible by 2^{M-u}, which is impossible, since $j - i < 2^{M-u}$. So we see that the number of distinct values of $S_j(\alpha)F2^u$ is equal to the total number of multiples of 2^u in J_M; so that all these values occur just once in every period, and they are equally-spaced with spacing 2^u.

(B)(iii) $t + 1 = c$: period $2^{M-c} = 2^{M-t-1}$. This equals the total number of odd multiples of 2^t in J_M; so each of them occurs just once in each period, and the values are equally-spaced with spacing 2^{t+1}.

(B)(iv) $t \geq c$: period 2^{M-c}. As has been explained, the values of the x_j alternate between odd and even multiples of 2^c. Since the total number of multiples of 2 in is just equal to the period, each value occurs just once in every period, and the values are equally-spaced with spacing 2^c.∎

Corollary 1: *Under the conditions of Theorems 1 and 2, the values generated have the following spacing:*

(Case A) $c = 0$: *spacing* 1;

(Case B) $c \geq 1$, *(i)* $t + 2 < c$: *spacing* 2^{t+2};

(ii) $t + 2 = c$: *spacing* 2^{u};

(iii) $t + 1 = c$: *spacing* 2^{t+1};

(iv) $t \geq c$: *spacing* 2^{c}.

[The equally-spaced points have spacings evaluated in the proof of Theorem 2. Note that, in every case,

$$SPACING = 2^{M} / PERIOD; \tag{33}$$

as must necessarily be the case, since there are 2^{M} integers in $J_{M} = [0, 2^{M})$.]

The property of equal spacing of values in a period is highly desirable in pseudo-random generators, and will be called ***uniformity***.

3. FAMILIES OF INDEPENDENT GENERATORS

Now consider several generators of type (2):

$$x_{j+1}^{(\nu)} \equiv a^{(\nu)} x_j^{(\nu)} + b^{(\nu)} \pmod{2^{M}}, \tag{34}$$

with $\nu = 1, 2, 3, \ldots$ Define

$$\alpha_{\mu\nu} \equiv a^{(\mu)} - a^{(\nu)}, \quad \beta_{\mu\nu} \equiv b^{(\mu)} - b^{(\nu)}, \tag{35}$$

and

$$\delta_{\mu\nu j} \equiv x_j^{(\mu)} - x_j^{(\nu)}, \tag{36}$$

reduced modulo 2^{M} (so that a negative difference becomes incremented by 2^{M}). If we apply (2) to (34) - (36), we get that

$$\delta_{\mu\nu(j+1)} \equiv \alpha_{\mu\nu} x_j^{(\mu)} + a^{(\nu)} \delta_{\mu\nu j} + \beta_{\mu\nu} \pmod{2^{M}}. \tag{37}$$

We see from this that, if, as we shall henceforth here assume,

$$(\forall \nu)\ a^{(\nu)} = a, \quad \text{so that} \quad (\forall \mu,\nu)\ \alpha_{\mu\nu} = 0, \tag{38}$$

then we have $$\delta_{\mu\nu(j+1)} \equiv a\delta_{\mu\nu j} + \beta_{\mu\nu} \pmod{2^M}, \tag{39}$$

which is exactly of the form (2); so that we may apply Theorems 1 and 2 to the resulting sequence of differences $[\delta_{\mu\nu j}]_{j=0}^{\infty}$.

For each pseudo-random sequence, we maximize uniformity and the length of the period by adopting the conditions (16) and

$$b \equiv 1 \pmod 2, \tag{40}$$

i.e., making a and b *odd*. The period is then of length 2^M (maximal) and the spacing of the equally-spaced values is then 1 (optimal uniformity).

Theorems 1 and 2 tell us that the differences $\delta_{\mu\nu j}$ will also exhibit uniformity, but we cannot get the best result, that of Case A, since now every $\beta_{\mu\nu}$ is *even*, being the difference of two odd numbers: this is Case B, with $c \geqslant 1$.

When the differences between two pseudo-random sequences exhibit uniformity, this shows a kind of 'incoherence' between the two sequences, and this clearly desirable property, which mimics, to some extent, statistical independence, will be called ***independence*** here.

Corollary 2: *All pseudo-random sequences satisfying* (2) *and* (16) *exhibit uniformity; families of such sequences satisfying* (34) - (40) *exhibit independence.*

[This is a restatement of Theorems 1 and 2.]

Corollary 3: *The canonical pseudo-random sequences* (1) *formed from* (2) *with* (16) *have uniformity (measured by the fineness of the spacing of values*

occurring in every period) equal to the period of the sequence. Maximum uniformity is thus 2^M.

⟦The spacing of the values ξ_j is, by (1), 2^{-M} times the spacing of the x_j (called '*SPACING*' in (33)). By (33), this is therefore 1/*PERIOD*. Since we measure the degree of *uniformity* as the reciprocal of the spacing of the ξ_j, it follows that this is just equal to *PERIOD*, the length of the period of the sequence (1) or (2).⟧

Thus the uniformity of the sequences $[\xi_j^{(\nu)}]_{j=0}^{\infty}$ is maximal: 2^M. Note that Theorem 2 and its corollaries allow us to use Theorem 1 alone to determine the uniformity of the pseudo-random sequence $[\xi_j^{(\nu)}]_{j=0}^{\infty}$, or the independence of two such sequences, similarly.

Our procedure is as follows:

(I) At each step, we may choose to follow one of two *branches* of a random walk, which we shall call the *left* and *right* branches; thus random *lists* are replaced by *random* (*binary*) *trees* (later we shall extend consideration to trees of general degree). These are the structures that Warnock (WAR 83) calls 'tree-structured random walks'.

(II) At the start, or *root*, we initiate the sequence $[\xi_j^{(1)}]_{j=0}^{\infty}$ with $\xi_0^{(1)} = x_0^{(1)}/2^M$.

(III) We may number the nodes by *levels*; so that node N has as left-child the node $2N$, and as right-child the node numbered $2N + 1$. In binary notation, node $b_0b_1\ldots b_k$ has left-child $b_0b_1\ldots b_k0$ and right-child $b_0b_1\ldots b_k1$; the root is node 1 ($b_0 = 1$); and we see that k is the level of the node $\mathbf{N} = (b_0b_1\ldots b_k)_{\text{base } 2}$.

(IV) As we arrive at node N, we establish a *record* (N, u_N, v_N), where u_N is a parameter taking a value $b^{(\nu)}$, for some ν to be determined, and v_N is similarly a value $x_j^{(\nu)}$, for some j and the same ν, with the record $(1, b^{(1)}, x_0^{(1)})$ at the root-node.

(V) If we move to the left-child, node $2N$, we form the record

$$(2N, u_{2N}, v_{2N}) = (2N, u_N, av_N + u_N \pmod{2^M}); \qquad (41)$$

that is, we continue the sequence of the *same* random generator.

(VI) If we move to the right-child, node $2N + 1$, we form the record

$$(2N + 1, u_{2N+1}, v_{2N+1}) = (2N + 1, u_{2N+1}, av'_N + u_{2N+1} \pmod{2^M}); \qquad (42)$$

that is, we modify v_N to v'_N and adopt a *new* random generator, with a new parameter $u_{2N+1} = b^{(\mu)}$ for some different μ from ν.

What characterizes this procedure precisely is, of course, the way in which we transit from v_N to v'_N and from u_N to u_{2N+1}. But, in every case, so long as the generators we use are of type (2) and the congruences (16) and (40) apply to a and all the u_N, Theorems 1 and 2 ensure that the individual (left-branching) sequences are all uniform and that the separate generators are all independent, in the sense defined earlier.

In WAR 83, it is proposed that (in our notation) all u_N be the same, with the left branch representing the path of a given particle from any node. The right branch then represents the initiation of a new particle, with the step from v_N to v'_N being effected by a different generator, $v'_N \equiv a'v_N + b' \pmod{2^M}$. However, our theorems do not apply here. The paths of individual particles are, in fact, computed from different segments of

the same large period of a single generator. For perspective, we should consider that a typical value of M is

$$M = 48, \quad \text{so that} \quad 2^M = 2.8 \times 10^{14}, \tag{43}$$

and a typical usage of random numbers might be of the order of 10^4 to 10^6; so that, since disjoint segments of a period are pretty incoherent with each-other, it is reasonable to assume that Warnock's scheme may well work efficiently. However, no rigorous mathematical results have yet been obtained to support this conjecture.

4. SPECIFIC PROCEDURES

The general procedure we propose is given in the algorithm (I) - (VI) outlined above. As a first proposal, consider the simplest arrangement:

$$v'_N = v_N \quad \text{and} \quad u_{2N+1} = 2N + 1, \quad \text{with} \quad u_1 = 1. \tag{44}$$

The generators of the two sequences (of left branches) starting at nodes $2N$ and $2N + 1$ (presumably representing the histories of two particles coming from the same event) will have b-parameters of the form $(2r + 1)$ and $(2r + 1)2^k + 1$ (if node N is descended by a series of k left branches from a right-child or the root). The corresponding difference-generator (39) will have $\beta_{\mu\nu} \equiv (2r + 1)(2^k - 1) + 1 \pmod{2^M}$ $(k \geq 1)$ and $\delta_{\mu\nu 0} = \beta_{\mu\nu}$, by (41) and (42). Thus, $t = c$ and we are in Case B(iv) with independence measured by 2^{M-c}, by Corollary 3 applied to the difference sequence (independence is just uniformity of differences). We see that $\beta_{\mu\nu} \equiv (2r + 1)2^k - 2r$, so that, if nodes $2N$ and $2N + 1$ are at level h and node $2r + 1$ is at level $h - k$ (remember that the level of a node is the highest power of 2 which does not exceed the node number; so $2^{h-k} < 2r + 1 < 2^{h-k+1}$ and $2^h < (2r + 1)2^k + 1 < 2^{h+1}$, which is consistent), then at most 2^{h-k}

will divide $2r$. If we let $2r = R2^q$ with R odd, then $q \leq h - k$ and if $q = h - k$ then $2r = 2^{h-k}$, i.e., $R = 1$. Now (i) if $k > h - k$ (i.e., $2k > h$), then $c = q \leq h - k < h$; (ii) if $k = h - k$ (i.e., $2k = h$), then either $q = h - k$, when $2r = 2^{h-k} = 2^k$ and $\beta_{\mu\nu} \equiv (2^k + 1)2^k - 2^k = 2^{2k}$, so that $c = 2k = h$; or $q < h - k$, when $c = q < h$; (iii) if $k < h - k$ (i.e., $2k < h$) then either $q < k$ and $c = q < k < h$; or $q = k$ and $c = 2k < h$; or $k < q \leq h - k$, when $c = k < h$. That is, in all circumstances, $c \leq h$, and this bound is attained when and only when $h = 2k$ and $2r = 2^k$, or $h = k$ and $2r = 0$.

If we use the random tree as suggested, taking left branches to generate the histories of particles and branching to the right when we create a new particle, or perform equivalently in other problems, then the physical situation indicates that adjacent branches (such as are discussed above) should be most independent.

When we examine the other parts of Case B, we see that (iii) is bad (like (iv)) and (ii) is worse. We note that we have not yet taken the freedom of choosing the transition from v_N to v'_N. In general, $\delta_{\mu\nu 0} \equiv av'_N - av_N + \beta_{\mu\nu} \pmod{2^M}$, and, by the analog of (19), we can make $t = 0$, say, simply by forcing, for example

$$v'_N \equiv v_N + 1 \pmod{2^M}. \tag{45}$$

This yields the case (i) if $c \geq 3$, and this latter can be forced by taking

$$u_{2N+1} \equiv 8N + 1 \pmod{2^M}. \tag{46}$$

Now the independence is measured by 2^{M-2}, which is excellent, for adjacent branches. One remaining problem, which seems to have no easy solution, is that non-adjacent, but close, branches may well have large values of t, which may put us into (ii), (iii), or (iv).

Nevertheless, the procedure embodied in (45) and (46) is clearly a valuable and workable one. A discussion similar to that given for the first method indicates that the maximum value of c at level h is $h + 2$, not much worse than the previous bound of h. (The two b-parameters are now $8r + 1$ and $(2r + 1)2^{k+2} + 1$, whose difference is just four times the previous form.)

For n-fold branching, we may simply use the binary branching repeatedly, and this may be sufficient for routine purposes, to avoid many ad-hoc procedures. It is possible, of course, to number the nodes of an n-ary tree by levels, as described in (III). The obvious procedure is now to number the children of node N as $nN - (n - 2)$, $nN - (n - 3)$, ..., $nN - 1$, nN, $nN + 1$ (note that the children of $N + 1$ follow immediately after those of N). The analog of (44), the simplest scheme, is then:

$$\left.\begin{aligned} &(nN,\ u_{nN},\ v_{nN}) = (nN,\ u_N,\ av_N + u_N \pmod{2^M});\\ &(nN + j,\ u_{nN+j},\ v_{nN+j}) = (nN + j,\ u_{nN+j},\ av_N + u_{nN+j} \pmod{2^M}),\\ &\qquad\qquad \text{for } j = 2 - n,\ 3 - n,\ \ldots,\ -2,\ -1,\ +1;\\ \text{with}\quad &u_{nN+1} \equiv 3 + 2(n - 1)(N - 1) \pmod{2^M},\\ \text{and}\quad &u_{nN+j} \equiv 3 + 2(n - 1)N + 2j \pmod{2^M},\\ &\qquad\qquad \text{for } j = 2 - n,\ 3 - n,\ \ldots,\ -2,\ -1. \end{aligned}\right\} \tag{47}$$

It would seem unnecessary to complicate things further by adopting a form such as (45) and (46), when it would only improve things for one of the branches.

BIBLIOGRAPHY

BUS 62 N. P. Buslenko, D. I. Golenko, Yu. A. Shreider, I. M. Sobol', V. G. Sragovich, *The Method of Statistical Trials — The Monte Carlo Method.* Edited by Yu. A. Shreider; Fizmatgiz, Moscow, 1962 (in Russian); Elsevier, Amsterdam, 1964, 312 pp.; Pergamon Press, Oxford, 1966, 390 pp.

CAR 75 L. L. Carter, E. D. Cashwell, *Particle Transport Simulation with the Monte Carlo Method.* Technical Information Center, Energy Research and Development Administration, Oak Ridge, TN, 1975, 121 pp.

ERM 71 S. M. Ermakov, *The Monte Carlo Method and Contiguous Questions.* Nauka, Moscow; First Edition, 1971, 328 pp.; Second Edition, 1975, 472 pp.

FRA 63 J. N. Franklin, Deterministic simulation of random processes, *Math. Comp.* 17 (1963) 28-59.

GRE 65 M. Greenberger, Method in randomness, *Commun. ACM* 8 (1965) 177-179.

HAL 60 J. H. Halton, On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals, *Numer. Math.* 2 (1960) 84-90.

HAL 70 J. H. Halton, A retrospective and prospective survey of the Monte Carlo method, *SIAM Review* 12 (1970) 1-63.

HAL 72 J. H. Halton, Estimating the accuracy of quasi-Monte-Carlo integration, *Applications of Number Theory to Numerical Analysis.* Edited by S. K. Zaremba, Academic Press, New York, 1972, 345-360.

HAM 60 J. M. Hammersley, Monte Carlo methods for solving multivariable problems, *Ann. New York Acad. Sci.* 86 (1960) 844-874.

HAM 64 J. M. Hammersley, D. C. Handscomb, *Monte Carlo Methods*. Methuen, London; John Wiley, New York, 1964, 185 pp.

HUL 62 T. E. Hull, A. R. Dobell, Random number generators, *SIAM Review* 4 (1962) 230-254.

JAN 66 B. Jansson, *Random Number Generators*. Doctoral Thesis, Faculty of Mathematics and Natural Sciences, University of Stockholm, 1966, 205 pp. (Distributed by Almquist & Wiksell.)

KLE 75 J. P. C. Kleijnen, *Statistical Techniques in Simulation*. Marcel Dekker, New York; Part I, 1974, 300 pp.; Part II, 1975, 503 pp.

LEH 51 D. H. Lehmer, Mathematical methods in large-scale computing units, *Proc. Second Symposium on Large-Scale Digital Calculating Machinery, 1949*. Harvard, Cambridge, MA, 1951, 141-146.

NIE 78 H. Niederreiter, Quasi-Monte Carlo methods and pseudo-random numbers, *Bull. Amer. Math. Soc.* 84 (1978) 957-1041.

MAR 72 G. Marsaglia, The structure of linear congruential sequences, *Applications of Number Theory to Numerical Analysis*. Edited by S. K. Zaremba, Academic Press, New York, 1972, 249-285.

RUB 81 R. Y. Rubinstein, *Simulation and the Monte Carlo Method*. John Wiley, New York, 1981, 293 pp.

SOB 73 I. M. Sobol', *Monte Carlo Computational Methods*. Nauka, Moscow, 1973, 312 pp.

SPA 69 J. Spanier, E. M. Gelbard, *Monte Carlo Principles and Neutron Transport Problems*. Addison-Wesley, Reading, MA, 1969, 248 pp.

TAU 65 R. C. Tausworthe, Random numbers generated by linear recurrence modulo 2, *Math. Comp.* 19 (1965) 201-209.

WAR 83 T. T. Warnock, Synchronization of random number generators, *Congressus Numerantium* 37 (1983) 135-144.

YAK 77 S. J. Yakowitz, *Computational Probability and Simulation.* Addison-Wesley, Reading, MA, 1977, 262 pp.

ZAR 66 S. K. Zaremba, Good lattice points, discrepancy, and numerical integration, *Ann. Math. Pura Appl.* IV:73 (1966) 293-317.

ZAR 68 S. K. Zaremba, The mathematical basis of Monte Carlo and quasi-Monte Carlo methods, *SIAM Review* 10 (1968) 303-314.