MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 131
JULY 1975, PAGES 929–934

Multiply Schemes and Shuffling

By M. Rosenblatt*

Abstract. Multiply schemes are used as a model of a linear congruential scheme. It is suggested how the properties of linear congruential schemes as pseudo-random number generators might be improved by shuffling. Asymptotic frequencies of pairs and triples from multiply schemes are obtained.

1. Introduction. Multiply schemes have been suggested as an idealized model of linear congruential schemes ([1] and [2]) and have also been of interest in number theory. It has been suggested that the properties of linear congruential schemes as pseudo-random number generators might be improved by shuffling (see [4] and [3]). The asymptotic frequencies of pairs and triples from multiply schemes with a uniform initial distribution are obtained and it is shown how the asymptotic distribution of pairs is improved by a shuffling scheme. From a practical point of view such results are only suggestive since they hold for "almost every initial choice" (with respect to the uniform distribution) in an idealized model.

2. Multiply Schemes. We first consider the sequence

$$x_{n+1} = Nx_n \quad \text{modulo } 1, \qquad n = 0, 1, 2, \ldots, \tag{1}$$

with $N > 1$ an integer. This can be considered an idealized model of the linear congruential scheme since it assumes unlimited accuracy in that x_n can be any real number $0 \leqslant x_n \leqslant 1$. Also, the uniform measure on $[0, 1]$ is an invariant measure with respect to the transformation $y = Nx$ modulo one, and we shall take x_0 with that initial distribution. Let

$$i[x_n \leqslant u_0, \ldots, x_{n+k} \leqslant u_k] = \begin{cases} 1 & \text{if } x_n \leqslant u_0, \ldots, x_{n+k} \leqslant u_k, \\ 0 & \text{otherwise.} \end{cases} \tag{2'}$$

We are interested in the asymptotic behavior as $n \longrightarrow \infty$ of the relative frequencies

$$\frac{1}{n}\sum_{j=1}^{n-1} i[x_j \leqslant u_0, x_{j+1} \leqslant u_1], \tag{2''}$$
$$\frac{1}{n}\sum_{j=1}^{n-2} i[x_j \leqslant u_0, x_{j+1} \leqslant u_1, x_{j+2} \leqslant u_2],$$

and seeing how this deviates from what one requires of a scheme ideally simulating random numbers, that is, u_0u_1 and $u_0u_1u_2$, respectively, where $0 \leqslant u_i \leqslant 1$.

Received March 18, 1974.

AMS (MOS) subject classifications (1970). Primary 10K05, 65C10, 62E25; Secondary 65C05.

Key words and phrases. Multiply scheme, shuffling, linear congruential scheme, pseudo-random number, uniform distribution, asymptotic frequency.

*Research supported by the Office of Naval Research.

The ergodicity of (1) with invariant uniform measure (for x_0) implies the existence of "time averages" and the equality of "time averages" with "space averages." This yields the old result on equidistribution that

$$\lim_{n\to\infty} \frac{1}{n}\sum_{j=1}^{n} i[x_j \leqslant u] = u \tag{3}$$

for almost every initial value x_0, $0 \leqslant u \leqslant 1$. The same type of argument can be used to determine the asymptotic behavior of (2′) and (2″). We first consider (2′) in the following lemma.

LEMMA 1. *Consider the sequence* (1) *with initial uniform distribution for* x_0. *Then, if* $0 \leqslant a, b \leqslant 1$,

$$\lim_{n\to\infty} \frac{1}{n}\sum_{j=1}^{n-1} i[x_j \leqslant a, x_{j+1} \leqslant b] = \frac{[Na]}{N}b + \frac{\min(\{Na\}, b)}{N} \tag{4}$$

for almost every initial value x_0, *where* $[u]$ *is the greatest integer less than or equal to* u *and* $\{u\} = u - [u]$.

From the remarks made earlier, the ergodicity of the sequence implies that the limit (4) exists for almost every initial value and is equal to the space average. The space average is

$$\int_{0\leqslant x_0 \leqslant a; 0 \leqslant \{Nx_0\} \leqslant b} dx_0. \tag{5}$$

Let $a = k/N + \alpha/N$ with k an integer, $0 \leqslant k < N$, and $0 \leqslant \alpha \leqslant 1$. Then $0 \leqslant x_0 \leqslant a$, $0 \leqslant \{Nx_0\} \leqslant b$ if and only if

$$j/N \leqslant x_0 \leqslant (j + b)/N, \qquad j = 0, 1, \ldots, k-1,$$

or

$$k/N \leqslant x_0 \leqslant (k + \min(\alpha, b))/N.$$

Thus (5) equals

$$(k/N)b + (\min(\alpha, b))/N,$$

and we have the desired result. Notice that the deviation from what one would expect in the case of independence is of magnitude $O(1/N)$. The following corollary is immediate.

COROLLARY 1. *Under the assumptions of Lemma* 1

$$\lim_{n\to\infty} \frac{1}{n}\sum_{j=1}^{n-m} i[x_j \leqslant a, x_{j+m} \leqslant b] = \frac{[N^m a]}{N}b + \frac{\min(\{N^m a\}, b)}{N}, \tag{6}$$

$0 \leqslant a, b \leqslant 1$, *for almost every initial value* x_0.

A similar but somewhat more elaborate argument will now be given to obtain the following result on the asymptotic behavior of 3-tuples.

THEOREM 1. *Consider the sequence* (1) *with uniform distribution for* x_0. *Let* $0 \leqslant u, v, w \leqslant 1$ *with*

$$u = \frac{u_1}{N^a} + \frac{u_2}{N^{a+b}} + \frac{\alpha}{N^{a+b}}, \qquad v = \frac{v_1}{N^b} + \frac{\beta}{N^b}, \qquad w = \gamma, \tag{7}$$

where $u_1 = 0, 1, \ldots, N^a - 1$, $u_2 = 0, 1, \ldots, N^b - 1$, $v_1 = 0, 1, \ldots, N^b - 1$, $0 \leqslant \alpha, \beta, \gamma \leqslant 1$ *and* a, b *are positive integers. Then*

$$\begin{aligned} &\lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n-a-b} i[x_j \leqslant u, x_{j+a} \leqslant v, x_{j+a+b} \leqslant w] \\ &= \frac{u_1 v_1 \gamma}{N^{a+b}} + \frac{\min(u_2, v_1)\gamma}{N^{a+b}} + u_1 \frac{\min(\beta, \gamma)}{N^{a+b}} \\ &+ \frac{\min(\alpha, \gamma)}{N^{a+b}} h(u_2, v_1) + \frac{\min(\beta, \gamma)}{N^{a+b}} h(v_1, u_2) \\ &+ \frac{\min(\alpha, \beta, \gamma)}{N^{a+b}} \delta(v_1 - u_2) \end{aligned} \tag{8}$$

for almost every initial value x_0, *where*

$$h(u, v) = \begin{cases} 1 & \text{if } u < v, \\ 0 & \text{otherwise.} \end{cases}$$

The broad outlines of the argument are those of Lemma 1. The space average is

$$\int_{0 \leqslant x_0 \leqslant u; 0 \leqslant \{N^a x_0\} = x_a \leqslant v; 0 \leqslant \{N^b \{N^a x_0\}\} = x_{a+b} \leqslant w} dx_0. \tag{9}$$

First $0 \leqslant x_a \leqslant v$, $0 \leqslant x_{a+b} \leqslant w$ if and only if x_a is in

$$\bigcup_{j=0}^{v_1 - 1} \left(\frac{j}{N^b}, \frac{j + \gamma}{N^b} \right) \tag{10}$$

or

$$\left(\frac{v_1}{N^b}, \frac{v_1 + \min(\beta, \gamma)}{N^b} \right). \tag{11}$$

Consider one of the intervals $(j/N^b, (j + \gamma)/N^b) = I_j$, $0 \leqslant j < v_1$. Now $0 \leqslant x_0 \leqslant u$, $x_a \in I_j$ for some j with $0 \leqslant j < v_1$ when

$$x_0 \in \bigcup_{k=0}^{u_1 - 1} \left(\frac{k}{N^a} + \frac{j}{N^{a+b}}, \frac{k}{N^a} + \frac{j + \gamma}{N^{a+b}} \right), \tag{12}$$

$$x_0 \in \left(\frac{u_1}{N^a} + \frac{j}{N^{a+b}}, \frac{u_1}{N^a} + \frac{j + \gamma}{N^{a+b}} \right) \quad \text{if } 0 \leqslant j \leqslant u_2 - 1, v_1 - 1, \tag{13}$$

and

$$x_0 \in \left(\frac{u_1}{N^a} + \frac{u_2}{N^{a+b}}, \frac{u_1}{N^a} + \frac{u_2 + \min(\alpha, \gamma)}{N^{a+b}} \right), \tag{14}$$

if $j = u_2 < v_1$. The total contributions from (12), (13), and (14), respectively, to the space average are

$$\frac{u_1 v_1 \gamma}{N^{a+b}}, \frac{\min(u_2, v_1)\gamma}{N^{a+b}} \quad \text{and} \quad h(u_2, v_1) \frac{\min(\alpha, \gamma)}{N^{a+b}}.$$

Now we have to determine when $0 \leqslant x_0 \leqslant u$,

$$x_0 \in \left(\frac{v_1}{N^b}, \frac{v_1 + \min(\beta, \gamma)}{N^b}\right).$$

This will happen if

$$x_0 \in \bigcup_{k=0}^{u_1 - 1} \left(\frac{k}{N^a} + \frac{v_1}{N^{a+b}}, \frac{k}{N^a} + \frac{v_1 + \min(\beta, \gamma)}{N^{a+b}}\right), \tag{15}$$

$$x_0 \in \left(\frac{u_1}{N^a} + \frac{v_1}{N^{a+b}}, \frac{u_1}{N^a} + \frac{v_1 + \min(\beta, \gamma)}{N^{a+b}}\right) \quad \text{if } u_2 > v_1, \tag{16}$$

$$x_0 \in \left(\frac{u_1}{N^a} + \frac{v_1}{N^{a+b}}, \frac{u_1}{N^a} + \frac{v_1 + \min(\alpha, \beta, \gamma)}{N^{a+b}}\right), \tag{17}$$

if $u_2 = v_1$. The contributions to the space average from (15), (16), and (17), respectively, are

$$\frac{u_1}{N^{a+b}} \min(\beta, \gamma), \quad h(v_1, u_2) \frac{\min(\beta, \gamma)}{N^{a+b}} \quad \text{and} \quad \delta(u_2 - v_1) \frac{\min(\alpha, \beta, \gamma)}{N^{a+b}}.$$

The proof of the theorem is complete. Notice that here the deviation from what might be expected in the case of independence is $O(N^{-\min(a,b)})$.

3. Shuffling. We now consider constructing a scheme that is an idealization of what is done in shuffling. Let

$$x_{n+1} = Nx_n \quad \text{modulo } 1, \qquad y_{n+1} = Ny_n \quad \text{modulo } 1, \tag{18}$$

with $n = \cdots, -1, 0, 1, \ldots$. Assume that x_0 and y_0 are uniformly distributed on $[0, 1]$. It has already been noted that the uniform distribution is invariant under one transformation (1). Further let the joint distribution of x_0 and y_0 be the product distribution so that the sequences $\{x_n\}$ and $\{y_n\}$ are independent. Set up a "table" with M locations

$$a_n(\cdot) = \{a_n(j); j = 0, 1, \ldots, M-1\}, \tag{19}$$

and if

$$y_{n+1} \in I_j = [j/M, (j+1)/M), \tag{20}$$

set

$$a_{n+1}(k) = a_n(k) \quad \text{if } k \neq j, \qquad a_{n+1}(j) = x_{n+1}, \tag{21}$$

and

$$z_{n+1} = a_n(j). \tag{22}$$

We assume that both N, M are large but that N is much larger than M is. The scheme $\{x_n, y_n, a_n(\cdot), z_n; n = \cdots, -1, 0, 1, \ldots\}$ we shall refer to as a "shuffling" scheme. The object of this section is to see in what way the sequence $\{z_n\}$ (at least for pairs z_n, z_{n+1}) simulates what one expects from a random-number sequence and contrasts with what was obtained in the last section for the sequence $\{x_n\}$. The following two lemmas are immediate.

LEMMA 2. *Given any invariant distribution v for (x_0, y_0) under* (18), *there is a corresponding invariant distribution for the "shuffling" scheme $\{x_n, y_n, a_n(\cdot), z_n\}$ unde* (20), (21), *and* (22) *with the given distribution v the marginal distribution for (x_0, y_0).*

LEMMA 3. *Consider the stationary "shuffling" scheme $\{x_n, y_n, a_n(\cdot), z_n\}$ with x_0, y_0 independent and uniformly distributed on* $[0, 1]$. *Then z_n is uniformly distributed on* $[0, 1]$.

Let

$$\begin{aligned} A_\alpha &= \{y_n, y_{n-1}, y_{n-2} \in I_\alpha\}, \\ B_{\alpha,\beta,j} &= \{y_n \in I_\alpha, y_{n-1} \in I_\beta; y_{n-2}, y_{n-3}, \ldots, y_{n-j-1} \notin I_\alpha, I_\beta; \\ &\qquad\qquad y_{n-j-2} \in I_\alpha, y_{n-j-3} \in I_\beta\}, \\ C_{\alpha,\beta,j} &= \{y_n \in I_\alpha, y_{n-1} \in I_\beta; y_{n-2}, y_{n-3}, \ldots, y_{n-j-1} \notin I_\alpha, I_\beta; \\ &\qquad\qquad y_{n-j-2} \in I_\beta, y_{n-j-3} \in I_\alpha\}. \end{aligned} \tag{23}$$

A few simple estimates lead to the following result.

LEMMA 4. *Let m be the measure of the stationary "shuffling" scheme $\{x_n, y_n, a_n(\cdot), z_n\}$ with x_0, y_0 independent and uniformly distributed on* $[0, 1]$. *Then*

$$m(A_\alpha) \leqslant \left(\frac{1}{M} + \frac{2}{N}\right)^3 \tag{24}$$

and

$$m(B_{\alpha,\beta,j}),\ m(C_{\alpha,\beta,j}) \leqslant \left(\frac{1}{M} + \frac{2}{N}\right)^4 \left(1 - \frac{2}{M} + \frac{4}{N}\right)^j. \tag{25}$$

It is enough to obtain the desired estimate for $m(B_{\alpha,\beta,j})$ since the argument required for the other estimates is similar. Now

$$\begin{aligned} B_{\alpha,\beta,j} \subset B = \{&y_n, y_{n-j-2} \in ([\alpha N/M]/N,\ ([(\alpha + 1)N/M] + 1)/N) \\ &y_{n-1}, y_{n-j-3} \in ([\beta N/M]/N,\ ([(\beta + 1)N/M] + 1)/N) \\ &y_{n-2}, \ldots, y_{n-j-1} \notin (([\alpha N/M] + 1)/N,\ [(\alpha + 1)N/M]/N), \\ &\qquad\qquad (([\beta N/M] + 1)/N,\ [(\beta + 1)N/M]/N)\} \end{aligned}$$

and the set B is determined by conditions on a finite number of the N-ary digits and these are independent. Thus

$$\begin{aligned} m(B) &= (m\{y_n \in ([\alpha N/M]/N,\ ([(\alpha + 1)N/M] + 1)/N)\})^2 \\ &\quad (m\{y_n \in ([\beta N/M]/N,\ ([(\beta + 1)N/M] + 1)/N)\})^2 \\ &\quad (m\{y_n \notin (([\alpha N/M] + 1)/N,\ [(\alpha + 1)N/M]/N), \\ &\qquad\qquad (([\beta N/M] + 1)/N,\ [(\beta + 1)N/M]/N)\})^j \\ &\leqslant \left(\frac{1}{M} + \frac{2}{N}\right)^4 \left(1 - \frac{2}{M} + \frac{4}{N}\right)^j. \end{aligned}$$

The estimates of Lemma 4 lead to the following theorem.

THEOREM 2. *Consider the stationary "multiply" scheme with x_0, y_0 independent and uniformly distributed on* $[0, 1]$. *Then*

$$|m\{z_{n-1} \leqslant u,\ z_n \leqslant v\} - uv| \leqslant C\frac{1}{MN} \tag{26}$$

if $0 \leqslant u, v \leqslant 1$, *with the constant* $C \leqslant 3$ *if* N *is sufficiently large relative to* M.

Now

$$\begin{aligned} &m\{z_{n-1} \leqslant u,\ z_n \leqslant v\} \\ &\quad = \left(\sum_{|k-j|=1} + \sum_{|k-j|>1}\right) m\{z_{n-1} = x_{n-j} \leqslant u,\ z_n = x_{n-k} \leqslant v\} \end{aligned} \tag{27}$$

and

$$\begin{aligned} &m\{z_{n-1} = x_{n-j} \leqslant u,\ z_n = x_{n-k} \leqslant v\} \\ &\quad = m\{z_{n-1} = x_{n-j},\ z_n = x_{n-k}\}\, m\{z_{n-1} \leqslant u,\ z_n \leqslant v | z_{n-1} = x_{n-j},\ z_n = x_{n-k}\} \end{aligned}$$

($m(A|B)$ denotes the conditional measure of the set A given set B) and

$$m\{z_{n-1} \leqslant u,\ z_n \leqslant v | z_{n-1} = x_{n-j},\ z_n = x_{n-k}\} = m\{x_{n-j} \leqslant u,\ x_{n-k} \leqslant v\}. \tag{28}$$

From (6) we know that $|m\{x_{n-j} \leqslant u,\ x_{n-k} \leqslant v\} - uv|$ is less than $1/N$ if $|k - j| = 1$ and less than $1/N^2$ if $|k - j| > 1$. Further (27) and (28) imply that

$$|m\{z_{n-1} \leqslant u,\ z_n \leqslant v\} - uv| \leqslant \left\{M^2\left(\frac{1}{M} + \frac{2}{N}\right)^3 + 2M^2\left(\frac{1}{M} + \frac{2}{N}\right)^4 \frac{M}{2 - 4M/N}\frac{1}{N}\right\}.$$

As a final remark we note that under the assumption of Theorem 2, the sequence $\{z_n\}$ is ergodic and so

$$\frac{1}{n}\sum_{j=1}^{n-1} i[z_j \leqslant u,\ z_{j+1} \leqslant v] \longrightarrow m\{z_1 \leqslant u,\ z_2 \leqslant v\}$$

as $n \longrightarrow \infty$ for almost every x_0, y_0.

Department of Mathematics
University of California, San Diego
La Jolla, California 92037

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

2. D. E. KNUTH, *The Art of Computer Programming.* Vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969. MR **44** #3531.

3. G. P. LEARMONTH & P. A. W. LEWIS, *Statistical Test of Some Widely Used and Recently Proposed Uniform Random Number Generators*, Proc. Conf. on Comput. Sci. and Statistics, Western Periodicals Co., North Hollvwood, Calif., 1973, pp. 163–171.

4. G. MARSAGLIA & T. A. BRAY, "One-line random number generators and their use in combinations," *Comm. ACM*, v. 11, 1968, pp. 757–759. MR 39 #5040.