An *A Priori* Determination of Serial Correlation in Computer Generated Random Numbers

By Martin Greenberger

1. Background. Ever since John Von Neumann introduced the "mid-square" method some ten years ago [11], users of "pseudo-random" numbers on modern digital computers have been generating their numbers as they were required in application, rather than drawing them from a table formed beforehand or obtaining them from a special-purpose device built expressly for this service. The advantages of Von Neumann's method were its speed, minimal storage requirements, and ability to be restarted from any desired point.

For some years now the mid-square method has been replaced by other recursive methods which have increased further the advantages of this general technique of generation. The most popular of these has been the "multiplicative congruential" method proposed by Lehmer in 1951 [2]. An interesting variation of this method, which we may call the "mixed congruential" method, recently has received the attention of several authors [1, 9, 10]. We adopt the notation of Coveyou, one of these authors. The mixed congruential method then may be written

$$x_{n+1} \equiv \lambda x_n + \mu \pmod{P}. \tag{1}$$

Here the modulus P generally equals one more than the largest (fixed-point) integer which the computer can store. The multiplier λ and the addend (or increment) μ are, to a degree, optional parameters of the generator; both parameters are positive integers less than P and relatively prime to P. The starting value x_0 is the first term of the integer sequence $\{x_n : 0 \leqq x_n < P(n = 0, 1, 2, \cdots)\}$ generated recursively by equation (1). And the numbers $\{x_n/P\}$ are the desired uniformly distributed drawings from the unit interval. For the special case of $\mu = 0$, equation (1) becomes the familiar multiplicative congruential method.

2. Selection of Parameters. It is not difficult to find values of the parameters λ and μ which produce a maximum period in the $\{x_n\}$ sequence for a given P [3–8, 10]. When P is a power of 2, for example, any odd μ combined with any $\lambda \equiv 1$ modulo 4 affords the maximum period, equal to P. For $\mu = 0$, the maximum period is reduced to $P/4$ and is attainable again with half the odd λ, now $\lambda \equiv 3$ or 5 modulo 8 [10].

Length of period is one standard that has been used in the selection of parameters; speed of generation is a second [1, 3, 4, 10]. But a great deal of freedom still remains, and the question of how best to use this freedom never has been fully answered. The most frequent solution has been to make a choice of parameters

Received June 27, 1960; revised February 10, 1961.

which appears favorable on intuitive grounds*, and then carefully examine generated subsequences by the standard statistical tests for serial correlations, runs, interval frequencies, and so on.

If we had a complete understanding of the relationship between the number theoretic properties of λ, μ, and P, on the one hand, and the statistical properties of the sequence they generate, on the other, the selection problem essentially would be solved. The fact is that we are still a considerable distance from having this complete understanding. Some recent work [9], however, has provided a start in the right general direction. We set out now, first to comment on this work, and then to develop some additional results which will help in the choice of generator parameters.

3. Serial Correlation. In his article on "Serial Correlation in the Generation of Pseudo-random Numbers" [9], Coveyou gives the following *approximate* formula for the serial correlation, $\rho(x_n, x_{n+1})$, between a number and its immediate successor in a full $\{x_n\}$ sequence generated by equation (1). (The symbol $\doteq$ denotes "approximately equal to").

$$\rho(x_n, x_{n+1}) \doteq \frac{1}{\lambda} - \frac{6\mu}{\lambda P}\left(1 - \frac{\mu}{P}\right) \tag{2}$$

Equation (2) is a good approximation to $\rho(x_n, x_{n+1})$ for λ small compared to $P^{1/2}$. For λ on the order of $P^{1/2}$ or larger, however, the approximation can fail badly, as an example will illustrate.

For $P = 2^{35}$, $\lambda = 2^{34} + 1$, and $\mu = 1$, the correlation given by equation (2) is a negligible 2^{-34}. The true correlation, however, is found by direct calculation to be a very significant .25, much too large to be acceptable. This is explained by the fact that values of λ which are very large relative to P have an effect similar to that of values of λ which are very small relative to P. This fact is completely distorted by the erroneous implication of equation (2) that the larger λ, the smaller the magnitude of the correlation.

As a consequence, the usefulness of equation (2) as a standard for selecting parameter values is limited. In what follows, an exact derivation of $\rho(x_n, x_{n+1})$ will provide us with a correction term for equation (2) which overcomes this limitation. The derivation begins along the same general lines as Coveyou's skillful approach.

4. Derivation. We shall assume throughout the derivation that λ and μ are restricted to values for which the period of the $\{x_n\}$ sequence is P. The sequence therefore will consist of all integers from 0 to $P - 1$ (chaotically disordered), with each integer appearing exactly once. Let the symbol E designate an expected or mean value over the full sequence. Then $\rho(x_n, x_{n+1})$ may be expressed as follows:

$$\rho(x_n, x_{n+1}) = \frac{E(x_n, x_{n+1}) - [E(x_n)]^2}{E(x_n^2) - [E(x_n)]^2} \tag{3}$$

where

$$E(x_n) = \frac{1}{P}\sum_{x=0}^{P-1} x = \frac{(P-1)}{2} \tag{4}$$

* One line of intuitive reasoning has led to a proposal that λ be on the order of $P^{1/2}$ [3, 4].

$$E(x_n^2) = \frac{1}{P}\sum_{x=0}^{P-1} x^2 = \frac{(P-1)(2P-1)}{6}. \tag{5}$$

To evaluate $E(x_n, x_{n+1})$, we equate x_{n+1} with the remainder r_n in the following equation

$$\lambda x_n + \mu = q_n P + r_n \qquad (n = 0, 1, \cdots) \tag{6}$$

where q_n and $r_n < P$ are non-negative integers, uniquely determined for each x_n by the Euclidean algorithm. Dispensing with the subscript n in equation (6) for convenience, we now may write

$$\begin{aligned} E(x_n, x_{n+1}) &= \frac{1}{P}\sum_{x_n=0}^{P-1} x_n x_{n+1} = \frac{1}{P}\sum_{x=0}^{P-1} x(\lambda x + \mu - qP) \\ &= \lambda E(x^2) + \mu E(x) - \sum_{x=0}^{P-1} xq. \end{aligned} \tag{7}$$

Assume for the moment that $\mu \geqq \lambda$ and let x_n, or x, in equation (6) take on consecutive integral values starting with 0. Then q increases from 0 to λ, in increments of 1, and each q has associated with it approximately P/λ consecutive integers x, as well as the same number of integers r. Let $\bar{r}_q$ be the smallest r associated with a given q. Then $\bar{r}_0 = \mu$, and for $q \geqq 1$, $\bar{r}_q < \lambda$ is given by

$$\bar{r}_q \equiv \mu - qP \pmod{\lambda}. \tag{8}$$

From this it follows that the $\bar{r}_q$ are distinct and $(\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_\lambda)$ is a permutation of the integers $(0, 1, \cdots, \lambda - 1)$.

It may be shown that

$$\begin{aligned} \sum_{x=0}^{P-1} xq = {} & \frac{\lambda P^2}{2} - \frac{\lambda P}{2} - \frac{\mu^2}{2\lambda} - \frac{\mu}{2} - \frac{P^2}{2\lambda^2}\sum_{\lambda q=} q^2 + \frac{(\lambda + 2\mu)P}{2\lambda^2}\sum_{q=1}^{\lambda} q \\ & - \frac{1}{2\lambda^2}\sum_{q=1}^{\lambda} \bar{r}_q^2 + \frac{\lambda + 2\mu}{2\lambda^2}\sum_{q=1}^{\lambda} \bar{r}_q - \frac{P}{\lambda^2}\sum_{q=1}^{\lambda} \bar{r}_q q \end{aligned} \tag{9}$$

and hence that

$$\begin{aligned} \sum_{x=0}^{P-1} xq = {} & \frac{\lambda P^2}{3} - \frac{\lambda P}{4} - \frac{\mu^2}{2\lambda} + \frac{P}{4} - \frac{\mu}{2\lambda} + \frac{\mu P}{2\lambda} + \frac{\lambda}{12} \\ & + \frac{\mu P}{2} - \frac{1}{12\lambda} - \frac{P^2}{4} - \frac{P^2}{12\lambda} - \frac{PS}{\lambda^2} \end{aligned} \tag{10}$$

where

$$S = \sum_{q=1}^{\lambda} \bar{r}_q q. \tag{11}$$

5. An Exact Formula for ρ. By combining equations (3, 4, 5, 7, and 10), we may now write a formula for $\rho(x_n, x_{n+1})$. In so doing we make the assumption that P is so large that any term whose order of magnitude is $1/P$ or less is negligible. This assumption leads to

$$\rho(x_n, x_{n+1}) \doteq \frac{1}{\lambda} - \frac{6\mu}{\lambda P}\left(1 - \frac{\mu}{P}\right) + \frac{12}{P}\left(\frac{S}{\lambda^2} - \frac{\lambda}{4}\right). \tag{12}$$

Since P is generally at least one billion, the approximation ($\doteq$) is an equality for all practical purposes.

The first two terms of equation (12) are seen to agree exactly with the approximation for ρ, equation (2), given earlier. The final term of equation (12) thus constitutes a correction to the earlier result, and it will be interesting to examine this term carefully. It is not difficult to show that

$$\frac{\lambda}{6}(\lambda^2 - 1) \leqq S \leqq \frac{\lambda}{3}(\lambda^2 - 1) \tag{13}$$

and hence, because of the magnitude of P,

$$-\frac{\lambda}{P} \leqq \frac{12}{P}\left(\frac{S}{\lambda^2} - \frac{\lambda}{4}\right) \leqq \frac{\lambda}{P}. \tag{14}$$

Thus, the correction term is confined to an interval extending a distance λ/P on either side of zero. At the mid-point of the interval, when the correction term equals zero, equation (12) reduces to equation (2). Equation (2) also suffices when λ is small relative to $P^{1/2}$, or more precisely, when $\lambda/P \ll 1/\lambda$. But for λ on the order of $P^{1/2}$ or larger, the correction term may predominate and the complete equation (12) must be used.

If we repeat the line of reasoning leading to equation (12) for the case $\mu < \lambda$, we find that

$$\rho(x_n, x_{n+1}) \doteq \frac{1}{\lambda} + \frac{12}{P}\left(\frac{S}{\lambda^2} - \frac{\lambda}{4}\right) \tag{15}$$

where

$$S = \sum_{q=1}^{\lambda-1} \bar{r}_q q \tag{16}$$

and inequality (14) again obtains. In a strict sense the notation should be modified to distinguish the S of equation (16) from the S of equation (11). However, the context (i.e., whether $\mu \geqq \lambda$ or $\mu < \lambda$) always identifies which of the definitions for S applies, and, in any case, the two definitions cannot give results for ρ different by more than a negligible amount. The implication of equation (15) is that equation (12) still applies for the case of $\mu < \lambda$. For this case, however, the middle term is insignificant and the parameter μ appears only insofar as it influences the value of S.

6. Examples and Applications. To evaluate S for some specific cases, let U be the unique non-negative integer less than λ for which

$$U \equiv \mu \pmod{\lambda} \tag{17}$$

and let

$$V = \frac{U}{\lambda} < 1. \tag{18}$$

In what follows, μ is assumed to be a positive odd integer less than $P = 2^{35}$.

First, suppose that $\lambda = 2^{34} + 1$. Then it may be shown* that

$$S \doteq (V^2 - V + \tfrac{7}{6})2^{100}. \tag{19}$$

The referee has pointed out that equation (1) is the reciprocity formula for Dedekind sums (after an elementary transformation). He has kindly supplied the reference to [12]. For V close to either 0 or 1 (e.g., $\mu = 1$), equation (19) leads to $S \doteq \frac{7}{6}2^{100}$ and the term involving S in equation (12) dominates. The other terms are negligible in comparison and equation (12) reduces to

$$\rho(x_n , x_{n+1}) \doteq \tfrac{12}{8}(\tfrac{7}{6} - 1) = \tfrac{1}{4} \tag{20}$$

which agrees with the result given earlier.

Next, suppose that $\lambda = 2^{18} + 1$. Then, if $U \leqq 2^{17}$,

$$S \doteq (-2V^2 + V + \tfrac{5}{12})2^{53} \tag{21}$$

whereas if $U > 2^{17}$,

$$S \doteq (-2V^2 + 3V - \tfrac{7}{12})2^{53}. \tag{22}$$

Equations (21) and (22) may be used with equation (12) to appraise different choices of μ. Let us examine $\mu = 1$ as an illustration. Then $U = 1$, $V \doteq 0$, $S \doteq (\frac{5}{12})2^{53}$, and

$$\rho(x_n , x_{n+1}) \doteq 2^{-18} + 12(2^{-18})(\tfrac{5}{12} - \tfrac{2}{4}) \doteq 2^{-18} - 2^{-18} \tag{23}$$

from which we infer that $\rho \ll 2^{-18}$.

It is not correct to conclude from this evidence alone, however, that a combination in equation (1) of $P = 2^{35}$, $\lambda = 2^{18} + 1$, and $\mu = 1$ furnishes an acceptable pseudo-random number generator. As a matter of fact, it does not [10]. For one thing, the first several hundred numbers generated by this combination, starting with $x_0 = 0$, are all less than $P/2$.

Now consider $\lambda = 2^{17} + 1$. With this λ,

$$S \doteq (-V^2 + V + \tfrac{5}{6})2^{49} \tag{24}$$

so that for V close to either 0 or 1, $S \doteq (\frac{5}{6})2^{49}$ and

$$\rho(x_n , x_{n+1}) \doteq 3(\mu^2 \cdot 2^{-67} - \mu \cdot 2^{-32} + 1)2^{-19}. \tag{25}$$

Thus, when $\mu = 1$, $\rho \doteq 3(2^{-19})$; and when μ simultaneously satisfies $\mu \doteq (1 \pm 2^{-1/2})2^{34}$ and $U \doteq 0$, $\rho \ll 2^{-19}$.

---

* In each of the examples discussed, special methods have been used to evaluate S, and the details are available upon request. The methods differ from each other somewhat, depending upon the values assumed by the parameters. It is actually possible to develop one general technique, a reciprocity type of reduction method, for solving all of the examples. S may be expressed in terms of an S', with $\lambda = P'$, by retracing many of the same steps which led to equation (12); and so on. The general technique has not yet proven as advantageous as the special methods in particular applications, but is of theoretical interest nonetheless. An elegant formulation of the general technique recently was developed by Coveyou in a private memorandum to the author.

Finally, consider λ sufficiently small relative to $P^{1/2}$ so that $\lambda/P \ll 1/\lambda$. Then inequality (14) indicates that the correction term in equation (12) is insignificant compared to $1/\lambda$ and therefore may be dropped. Consequently,

$$\rho(x_n, x_{n+1}) \doteq \frac{1}{\lambda}\left(\frac{6\mu^2}{P^2} - \frac{6\mu}{P} + 1\right). \tag{26}$$

It follows that $\rho \doteq 1/\lambda$ when $\mu \ll P$, whereas $\rho \ll 1/\lambda$ when $\mu \doteq P(1 \pm 3^{-1/2})/2$. Here λ and μ are restricted to values which afford the full period. One such selection of $P = 2^{35}$, namely $\lambda = 2^7 + 1$ and $\mu = 1$, has been tested empirically and proposed as a suitable generator [1].

7. Higher-Order Correlations. As is pointed out by Coveyou [9], equation (12) can be adapted to give correlations of the $\{x_n\}$ sequence with lags greater than 1. To accomplish this, we define non-negative integers λ_m and μ_m, both less than P, by the congruences

$$\lambda_m \equiv \lambda^m \quad \text{and} \quad \mu_m \equiv \frac{(\lambda^m - 1)\mu}{\lambda - 1} \pmod{P} \tag{27}$$

where $m = 1, 2, \cdots$. By applying equation (1) repeatedly, we may write

$$x_{n+m} \equiv \lambda_m x_n + \mu_m \pmod{P} \tag{28}$$

which is identical to equation (1) in the special case $m = 1$.

Equation (28) generates a sequence in which x_{n+m} is the immediate successor to x_n. If λ_m and μ_m are such as to make the period of this sequence P, then equation (12) with λ replaced by λ_m and μ replaced by μ_m may be used to evaluate $\rho(x_n, x_{n+m})$. This is then the correlation with lag m of the original $\{x_n\}$ sequence.

Thus, the evaluation of mth-order correlations introduces no new problems so long as the selection of λ and μ leads to pairs (λ_m, μ_m) which produce full periods. In this regard we note that with P a power of 2, μ odd, and $\lambda \equiv 1$ modulo 4,things work out well. For then μ_m is odd and $\lambda_m \equiv 1$ modulo 4 for every positive integer m. Thus, the sequence generated by equation (28) does have period P [10], and equation (12) may be used to calculate a serial correlation of any order.

Massachusetts Institute of Technology
Cambridge, Massachusetts

1. A. Rotenberg, "A new pseudo-random number generator," *J. Assoc. Comput. Mach.*, v. 7, 1960, p. 75–77.
2. D. H. Lehmer, "Mathematical methods in large scale computing units," Annals of the Computation Laboratory of Harvard University, v. 26, *Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery*, 1951, p. 141.
3. G. H. Orcutt, M. Greenberger, J. Korbel & A. M. Rivlin, *Microanalysis of Socio-economic Systems*, Appendix to Part IV, Harper & Bros., New York, 1961.
4. M. Greenberger, "Random number generators," Preprints of the 14th National Conference of the *ACM*, September 1959.
5. J. Todd & O. Taussky, "Generation of pseudo-random numbers," in *Symposium on Monte Carlo Methods*, H. A. Meyer, Editor, John Wiley & Sons, New York, 1956, p. 15–28.
6. M. L. Juncosa, "Random number generation on the BRL high-speed computing machines," Report No. 855, Ballistics Research Laboratories, Aberdeen Proving Ground, Maryland, 1953.
7. Eve Bofinger & V. J. Bofinger, "On a periodic property of pseudo-random sequences," *J. Assoc. Comput. Mach.*, v. 5, 1958, p. 261.

8. J. CERTAINE, "On sequences of pseudo-random numbers of maximal length," *J. Assoc. Comput. Mach.*, v. 5, 1958, p. 353.
9. R. R. COVEYOU, "Serial correlation in the generation of pseudo-random numbers," *J. Assoc. Comput. Mach.*, v. 7, 1960, p. 72–74.
10. M. GREENBERGER, "Notes on a new pseudo-random number generator," *J. Assoc. Comput. Mach.*, v. 8, 1961, p. 163.
11. A. S. HOUSEHOLDER, Editor, *Monte Carlo Method, Nat. Bur. Standards App. Math. Ser.* No. 12, June 1951, p. 33–37.
12. H. RADEMACHER & A. WHITEMAN, "Theorems on Dedekind sums," *Amer. J. Math.*, v. 63, 1941, p. 377–407.