Correlations in Power Residue Generated Random Numbers

The algebraic basis of harmful correlations in power residue generated random numbers is discussed. It is shown algebraically how to pick a multiplier to eliminate triplet correlations, and a set of multipliers is suggested to eliminate correlations in higher dimensions. Marsaglia's basis vector test for correlations is improved so it gives quantitative agreement with the algebraic method.

There are many problems in applied mathematics in which the solution is found by a "Monte Carlo" method involving the use of a long sequence of random numbers, uniformly distributed between 0 and 1. A frequently used method of generating such a sequence is the power residue method,

$$\begin{aligned} u_{n+1} &= (u_n * A)\ \mathrm{MOD}(M) \\ W_n &= u_n/M \end{aligned} \tag{1}$$

where A and M are integers, $u_1, u_2, \ldots$ is a sequence of integers, each of which is between 0 and $M - 1$, and $w_1, w_2, \ldots$ is a sequence of reals, each of which is between 1 and $1 - 1/M$. The sequence of w's may not give an accurate solution to the problem at hand if it contains correlations, so it is important to detect and eliminate correlations.

Our analysis of correlations is divided into two parts. The first deals with the cause of correlations in power residue generated random numbers from an algebraic point of view. It is shown how to pick values of A which do not have troublesome correlations in three dimensions, and a method is proposed to minimize the effects of correlations in higher dimensions. The second section deals with a method devised by G. Marsaglia [1] to test whether a given A, M produce a uniform density in the N-dimensional hypercube. An improvement is made so the test is more quantitatively accurate.

The Algebraic Basis of Correlations

The basic method of detecting correlations in a sequence of reals $y_1, y_2, \ldots$, with the y's uniformly distributed between 0 and 1 is to group successive y's in N-tuples and examine the distribution of points in the N-dimensional hypercube.

For example, the numbers of the sequence could be grouped in pairs, (y_1, y_2), (y_3, y_4),... with each pair representing a point in the unit square. If the y's are pairwise uncorrelated, i.e., if the y_{2n+2} is independent of y_{2n+1}, then the density of points will be uniform over the unit square. A nonuniform density indicates a correlation.

All power-residue-generated sequences of numbers fail the pairwise correlation test. That is, we can write

$$W_{n+2} = (W_{n+1} * A)\,\text{MOD}(1) \tag{2}$$

so that w_{n+2} is not only correlated with w_{n+1}, it is a function of it. Thus instead of having a uniform density in the unit square, the set of points (w_1, w_2), (w_3, w_4),... will fall only on a set of lines in the square. For example, if we choose $A = 5$, $M = 2^{31}$, so $w_{n+1} = (5w_n)$ MOD(1), then all pairs (w_n, w_{n+1}) fall on the lines $y = (5x)$ MOD(1), illustrated in Fig. 1. This type of slow oscillation in two dimensions is such a great departure from uniform density that $A = 5$, $M = 2^{31}$ is unacceptable for almost any application: A Monte Carlo integration in two dimensions would, in general, give quite inaccurate results, for example.

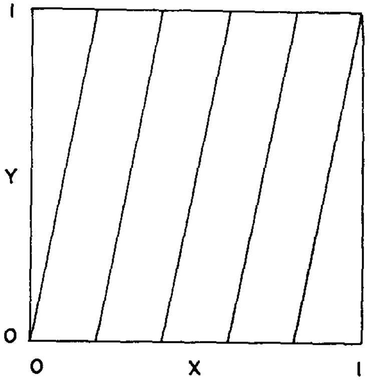

FIG. 1. A plot of $y = (5x)$ MOD(1) in the unit square. The random number generator $u_{n+1} = (5*u_n)$ MOD(2^{31}) produces "random" pairs of points, $(u_n/2^{31}, u_{n+1}/2^{31})$ which lie on the lines.

On the other hand, if A and M are large compared to 1, then the lines will be close together and from a "macroscopic" point of view, the density is essentially uniform. For example, in the IBM 360 subroutine RANDU [2], $A = 2^{16} + 3 = 65539$, $M = 2^{31}$, w_{n+2} oscillates from 0 to 1 65539 times while w_{n+1} goes from 0 to 1 once, so that on a scale of 1/1000, say, the density will appear uniform. One cannot get rid of this correlation, *but it is harmless for any reasonable problem.*

Consider next triplet correlations, i.e., form triplets of points (y_1, y_2, y_3), (y_4, y_5, y_6),..., each of which is a point in the unit cube. If the sequence of y's contains no correlations, then the points will have a uniform density in the unit cube, or conversely a nonuniform density represents a correlation.

It was found while doing a random walk in a two-dimensional lattice that RANDU has triplet correlations. If we represent w_{n+1} by x, w_{n+2} by y and w_{n+3} by z, then z is a function of x and y,

$$z = (6y - 9x) \text{ MOD}(1). \tag{3}$$

That is, the triplets fall on a set of planes in the unit cube and therefore are not uniformly distributed. As an example, we choose nine consecutive numbers generated by RANDU and group them in triplets, along with the above function.

x	y	z	$(6y - 9x)$ MOD(1)
0.3391	0.0345	0.1553	0.1553
0.6211	0.3290	0.3836	0.3836
0.3407	0.5918	0.4846	0.4846

In contrast to the rapidly oscillating pairwise correlations of RANDU, these triplet correlations oscillate slowly in the unit cube and could very easily cause problems in a Monte Carlo calculation. In fact, they caused a complete breakdown of the two-dimensional random walk problem where they were discovered.

Although it was found by trial and error, one can prove the relation (3) algebraically, using equation (1), with $A = 2^{16} + 3$, $M = 2^{31}$. Let

$$\begin{aligned} u_2 &= [(2^{16} + 3) * u_1] \text{ MOD}(2^{31}), \\ u_3 &= [(2^{16} + 3) * u_2] \text{ MOD}(2^{31}). \end{aligned} \tag{4}$$

Using modulo arithmetic to add and drop multiples of 2^{31}, we find

$$\begin{aligned} u_3 &= [(2^{16} + 3)^2 u_1] \text{ MOD}(2^{31}) \\ &= [6 * 2^{16} * u_1 + 9 * u_1] \text{ MOD}(2^{31}) \\ &= [6 * (2^{16} + 3) u_1 - 9u_1] \text{ MOD}(2^{31}) \\ &= (6 * u_2 - 9 * u_1) \text{ MOD}(2^{31}) \end{aligned} \tag{5}$$

and division by 2^{31} yields $w_3 = (6w_2 - 9w_1)$ MOD(1).

Since slow oscillations in 3 dimensions can cause difficulties, we would like a method for choosing values of A which do not have them. One procedure is to choose an A and apply Marsaglia's test to it. This method is not necessary to get rid of triplet correlations, however, because we can algebraically choose "good" values of A. Let

$$A = 2^{16} + C, \tag{6}$$

with C an integer. We then find

$$z = (2Cy - C^2x) \text{ MOD}(1). \tag{7}$$

Thus if C is large, on the order of 1000, say, then the $z(x, y)$ surface oscillates 2,000 times in the y direction in the unit cube, instead of six times as it did when C was three, while there are 1,000,000 oscillations instead of 9 in the x direction. A large value of C therefore produces triplet correlations which oscillate rapidly enough to make them harmless in most reasonable problems [3].

We can now give conditions for acceptable values of A and M. The optimum value of M is set by the computer so that modulo arithmetic is done automatically. If the computer stores an integer as a binary number with b digits ($b = 31$ for the IBM 360), then

$$M = 2^b. \tag{8}$$

The integer A must satisfy three conditions: first, in order to obtain the longest ($M/4$) nonrepeating sequence of random numbers [4], $A = \pm 3$ MOD(8); second, if u_{n+1} is to be as independent as possible of u_n, A should be of the order of [4, 5] $M^{1/2}$; and third, we should make the triplet correlations as innocuous as possible by causing the surface $z(x, y)$ to oscillate very rapidly as a function of x and y.

To satisfy the first two conditions, we set [6]

$$A = 2^n + C \tag{9a}$$

where n is the smallest integer greater than or equal to $b/2$, and where [7]

$$C \ll 2^n \tag{9b}$$

$$C = \pm 3 \text{ MOD}(8) \tag{9c}$$

We see from equation (7) that to make the oscillations rapid, we must choose

$$C \gg 1 \tag{9d}$$

For example, any of the 258 A's,

$$A = 2^{16} + 2^{10} + 3 + 8n = 66563 + 8m$$

or

$$A = 2^{16} + 2^{10} + 5 + 8n = 66565 + 8m \tag{10}$$

$$m = 0, 1, 2, \ldots, 2^7,$$

will give very fast, and therefore harmless, triplet correlations for $M = 2^{31}$ and would thus be suitable for problems where random points from the unit cube are used [8].

The algebraic detection of correlations in higher dimensions presents severe difficulties, and cannot readily be done [9]. If one must do a problem where higher order correlations are important, but you do not wish to go to the trouble of applying Marsaglia's test, then the following strategy is suggested. Suppose a sequence of L random numbers is needed. Generate the first $L/258$ of them using $A = 66563$, the second $L/258$ using $A = 66563 + 8$, etc. Each A will have its own oscillations in N dimensions, some slow [10], some fast. Since the oscillation frequencies for each are presumably different, the net result will be a reasonably uniform density.

Basis Vector Detection of Correlations

Marsaglia [1, 11] has devised a test which is supposed to show, with relatively little calculation, how uniform or nonuniform the density will be in N dimensions. The test, described very roughly, is as follows: A set of N basis vectors, each with integer components, is found such that all $(u_{n+1}, u_{n+2}, \ldots, u_{n+N})$ can be written as integer linear combinations of them. This basis is changed to a different basis by certain rules until an optimum basis is reached in which the new basis vectors, which we call BEST2 vectors (after the algorithm for calculating them), are as short and as orthogonal as possible, within the confines of integer components. The ratios of the lengths of the BEST2 vectors then, according to Marsaglia, give a measure of the uniformity of the density. Presumably the closer the ratios are to 1, the more uniform the density.

For example, the ratios [1] in the three dimensional cube for RANDU are 1:2:1819, which is very far from 1:1:1. And thus the test correctly predicts a nonuniform density in three dimensions for RANDU. But if the test is applied to $A = 4357$, $M = 2^{35}$ in two dimensions, the ratio [1] is 1:1810. And since this is superficially as "far" from nonuniformity (i.e., 1:1) as RANDU, we expect a highly nonuniform density in the unit square. Algebraically, however, we have $w_{n+1} = (w_n * 4357)\ \mathrm{MOD}(1)$, which is an extremely fast oscillation, and is harmless. An actual check [12] of the density also yielded no correlations.

Thus, Marsaglia's test is not quantitatively accurate. It can be made so, however, if some insight into the properties of the BEST2 vectors is gained. This is most easily done by looking at an example, and we choose $A = 5$, $M = 2^{14} = 4096$. Successive pairs (u_n, u_{n+1}) of points from the sequence $u_{n+1} = (5 * u_n)\ \mathrm{MOD}(4096)$ will be points in two dimensional space with integer components, where $0 < u_n < 4096$, $0 < u_{n+1} < 4096$. And we know from the algebra section that if the set of points $(u_n/4096, u_{n+1}/4096)$ is plotted in the unit square, Fig. 1 will result.

The original basis vectors for the sequence are (1,5) and (0,4096). That is, every (u_n, u_{n+1}) can be written as $c_1 * (1,5) + c_2 * (0,4096)$, with c_1, c_2 integer [13]. If the BEST2 algorithm is applied, the BEST2 basis vectors are $v_1 = (1,5)$ and $v_2 = (-788,156)$, and, again, every (u_n, u_{n+1}) can be written as a linear, integer combination of v_1 and v_2.

The set of all (u_n, u_{n+1}) generated by the sequence is (a subset of [13]) the set of all integer, linear combinations of v_1 and v_2 which fall within the square $0 < x < 4096$, $0 < y < 4096$. If we divide each of the components of v_1, v_2 by 4096, we can think of them as vectors in the unit square. $v_1/4096$ is very short and points in the direction of the lines of Fig. 1. $v_2/4096$ points in a direction perpendicular to the lines and its length, 0.196117, is very close to the distance between lines, 0.196116. Thus multiples of v_1 generate the points within a line in Fig. 1, while adding a multiple of v_2 induces a change from one line to another.

We can generalize the results to three dimensions. Let us suppose that A, M yield no slow oscillations in two dimensions, but do produce slow oscillations in three dimensions, so the points fall only on certain parallel planes in the unit cube. If we call the BEST2 vectors v_1, v_2, v_3, they will be (nearly) mutually orthogonal, with the longest, v_3, perpendicular to the planes. And the length of v_3, divided by M, will be the distance between planes. Our criterion for a uniform density in N dimensions is therefore: *If the length of the longest* BEST2 *vector in N dimensions is $d_{\max}$, then the density is uniform when $d_{\max}/M \ll 1$, but is nonuniform if $d_{\max}/M$ is near* 1.

How small $d_{\max}/M$ should be depends on the particular problem at hand. For some problems, a distance between planes of 1/20 would be sufficient, while more precise work may require 1/100, or even less.

We have seen that this criteria works in the simple case, $A = 5$, $M = 2^{14}$ and will now apply it to some of the other A, M investigated by Marsaglia. Consider first, $A = 4357$, $M = 2^{35}$. In place of a direct calculation of the BEST2 vectors, we can use the fact, given by Marsaglia, that the ratio of the lengths is 1:1810 and their product [14] is $M = 2^{35}$. This yields $d_{\max}/M = 2.29517 \times 10^{-4}$ while the actual distance between lines from the function $y = (4357x)$ MOD(1) is 2.29516×10^{-4}.

The test was also applied to RANDU in three dimensions. The BEST2 vectors were calculated and $d_{\max}/M$ was found to be 0.09205741. This compares favorably with the algebraically calculated value of $1/\text{SQRT}(9^2 + 6^2 + 1^2) = 0.09205741$. Both the algebraic method and basis vector test imply that RANDU does not produce a uniform density in three dimensions.

These examples indicate that our basis vector criterion is quantitatively accurate.

Marsaglia's criteria, that length ratios close to 1 imply a uniform density, is justified, as far as we know, only by appeal to our criteria. That is, length ratios close to 1 imply $d_{\max}/M \ll 1$ which implies a uniform density. For example, if we choose $M = 2^{35}$ and $N = 5$, and if we assume the BEST2 vectors are orthogonal and equal in length, then the product of the lengths, d, of the 5 vectors is M^4, so $d/M = M^{-1/5} = 1.0/2^7 = 0.0078$.

The application of our criteria to higher dimensions is interesting. Let us choose $M = 2^{35}$ and $N = 10$. The optimum case (minimum $d_{\max}/M$) is for the length ratios to be 1. Reference [12] then implies $d_{\max}/M$ cannot be less than $1/2^{3.5} = 0.09$. So, it looks like our criteria says there is a nonuniform density. On the other hand, $M = 2^{35}$ produces a sequence whose maximum length is 2^{33} and, in 10 dimensions, 2^{33} points give an average nearest neighbor distance of about 0.1. And a nonuniformity of $d_{\max}/M = 0.09$ is not bothersome when the nearest neighbor distance is about 0.1. We conclude that the test is still useful for "large" N, but one must use care in deciding what an acceptable value of $d_{\max}/M$ is.

REFERENCES

1. G. MARSAGLIA, "Applications of Number Theory to Numerical Analysis," (S. K. Zaremba Ed.) pp. 249–287, Academic Press, New York, 1972).
2. The same equation holds if we set $M = 2^b$ and $A = 2^n + C$, with b and n integers and $n \geqslant b/2$.
3. Reference [1] suggests 65549 as an alternative to 65539. This gives $C = 13$ so $z(x, y) = (26y - 169x)$ MOD(1), which is a sufficiently rapid oscillation for some purposes.
4. IBM CORP. "Random Number Generation and Testing," Reference Manual C20-8011, New York, 1959.
5. Although we have chosen to follow this suggestion, we do not regard it as necessary. A greater than or equal to 1000, say, will produce such rapid two dimensial oscillations that u_{n+1} is essentially independent of u_n.
6. Some random number generators "undershoot" $M^{\frac{1}{2}}$ instead of overshooting, as is done in Eq. (9a). As an example, take $u_{n+1} = [(2^{15} + 3) * u_n]$ MOD(2^{31}). This is no better than $2^{16} + 3$, because one can show, using the fact that u_n is odd, that $u_3 = (6u_2 - 9u_1 + 2^{30})$ MOD(2^{31}) or $z(x, y) = (6y - 9x + \frac{1}{2})$ MOD(1). A larger undershoot may produce a safe random number generator.
7. If C were on the order of 2^n, we might get slow oscillations in x, not directly predicted by Eq. (7).
8. Analogous results hold for other M's. For example, if $M = 10^{10}$, then A can be chosen as $10^5 + 10^3 + 3 + 10m$.
9. Note that it is the distance between planes (or hyperplanes) that determines how uniform the density is. Thus oscillations must be slow in every direction to have a bad A. For example, $z = (1000x - 3y)$ MOD(1) would not be considered slow.
10. If we consider A's from 2^{16} up to 2^{30}, say, with $M = 2^{31}$, very few give slow socillations in three dimensions. This leads us to believe that relatively few of the A's in equation (10) will have slow oscillations in 4, 5, 6,... dimensions.
11. Marsaglia also noticed that random numbers fall in planes. G. MARSAGLIA, *Proc. Nat. Acad. Sci.* **61**, 25 (1968); *Numer. Math.*, **16**, 8 (1970). He did not clearly distinguish, however, between slow, harmful oscillations, and fast, harmless oscillations, and gave no specific examples of slow oscillations.

12. 3200 pairs of random points were generated. Those falling in the lower left sixteenth of the unit square were plotted and no correlation was visible. This "eyeball" check is admittedly not definitive, but it certainly shows there are no pair correlations as severe as the triplet correlation in RANDU, for $A = 4357$, $M = 2^{35}$.
13. Not all multiples of the basis vectors are produced by the sequence (u_n, u_{n+1}). In the text example, $c_1 \equiv (u_1)$ MOD(8), where u_1 is the first value of u chosen, and is, of course, odd. See W. A. Beyer, "Applications of Number Theory to Numerical Analysis" (S. K. Zaremba, Ed.) pp. 361-370, Academic Press, New York, 1972 for a much fuller discussion of the related problem of the lattice structure and reduced bases for N-tuples generated by the power residue method.
14. The product of the lengths of the vectors is always greater than or equal to M^{N-1}. If they are assumed orthogonal, the product is equal to M^{N-1}.

Received: June 2, 1975

F. A. Blood, Jr.

Physics Department
Rutgers University
Camden College of Arts and Sciences
Camden, New Jersey 08102

Printed in Belgium