117622

DIRECTORATE OF MATHEMATICS AND STATISTICS

DMS STAFF NOTE NO. 18/75

TIME SERIES BEHAVIOUR OF THE IBM 360 AND IBM 1130 RANDOM NUMBER GENERATORS

BY

E.L. LEESE

OTTAWA, ONTARIO

SEPTEMBER 1975

ABSTRACT

This note examines the 'time series' properties of the random number sequences generated by the IBM Scientific Subroutine Package routine RANDU, for the IBM 360 and IBM 1130 computers, from the point of view of serial correlation at various lags from one to ten.

Analytical calculations show that for both computers the serial correlations are extremely small, for all lags from one to ten. The largest serial correlation for the IBM 360 is 0.000014, while the largest for the IBM 1130 is 0.00126.

TIME SERIES BEHAVIOUR OF THE IBM 360 AND IBM 1130 RANDOM NUMBER GENERATORS

Introduction

One of the programs in the IBM Scientific Subroutine Package for the IBM 360 and for the IBM 1130 computers (References (1) and (2)) is a random number generator RANDU.

In a recent issue of the magazine Datamation (Reference (3)), it was reported that Stanford University have decided to abandon the IBM Scientific Subroutine Package, partly because of the poor behaviour of sequences of random numbers generated by RANDU. It is alleged that 'consecutive triples of numbers are completely correlated'.

Since the meaning of this statement is not at all clear, we decided to have a look at the 'time series' properties of RANDU, by computing the serial correlations at lags 1,2,3,...10. To do this we followed the method suggested on pages 69-79 of Volume 2 of D.E. Knuth's 'The Art of Computer Programming' (Reference (4)).

In this note we explain the method of calculation of the serial correlations, and give the values obtained for both the IBM 360 and IBM 1130 versions of RANDU. (We point out a small error in one of Knuth's formulae).

Method of Calculation

For either the IBM 360 or the IBM 1130, RANDU generates random number sequences by repeated application of the recurrence

$$s(x) \equiv ax \pmod{M} \qquad (1)$$

where $a = 65539$ and $M = 2^{31} = 2147483648$ for the IBM 360 (2)

whereas $a = 899$ and $M = 2^{15} = 32768$ for the IBM 1130 (3)

Note that in each case <u>a and M have no common factors</u>.

You are supposed to start the sequence with an integer 'seed' which can be any odd number in (1,M-1). Since for either computer the value of a is of the form (4k+3) and M is a multiple of 4, we see that the numbers generated by (2) or (3) will be alternately of the form (4k+1), (4k+3), (4k+1), (4k+3), ...

We want to compute the serial correlation between x and its immediate successor s(x),

$$C_1 = \text{cov}\left[x, s(x)\right] \Big/ \sqrt{\text{var}(x) \ \text{var}\left[s(x)\right]} \tag{4}$$

where $\text{var}(x) = E(x^2) - \left[E(x)\right]^2$ (5)

$$\text{var}\left[s(x)\right] = E\left[\{s(x)\}^2\right] - \left[E\{s(x)\}\right]^2 \tag{6}$$

$$\text{cov}\left[x, s(x)\right] = E\left[xs(x)\right] - \left[E(x)\right] . \left[E\{s(x)\}\right] \tag{7}$$

To do so, we must make an assumption about the distribution of x. Although, as we have just mentioned, a given random number in the sequence must either be of the form (4k+1) or of the form (4k+3), it is usual to make a slight approximation and assume that x is equally likely to have any integer value in (0,M-1). (See, for example, Reference (4) page 72 equation (14)). We adopt this approximation here.

On this assumption, we have

$$E(x) = \frac{1}{M} \sum_{x=0}^{M-1} x = \frac{1}{2} (M-1) \tag{8}$$

and $E(x^2) = \frac{1}{M} \sum_{x=0}^{M-1} x^2 = \frac{1}{6} (M-1)(2M-1)$ (9)

Moreover, since a and M have no common factor, as x takes the values 0,1,2,...(M-1) the expression s(x) takes <u>each</u> of the values 0,1,2,...(M-1) <u>in some order</u>. For s(x) must always be an integer in (0,M-1). And if there were two integers, both in (0,M-1), say x_1 and x_2, for which $s(x_1) = s(x_2)$, equation (1) would tell us that (ax_1-ax_2) was a multiple of M, say

$$ax_1-ax_2 = KM \tag{10}$$

whence $$\frac{a}{M} = \frac{K}{x_1-x_2} \tag{11}$$

Since $|x_1-x_2| \leq M-1$, this would imply that the fraction a/M is not in its lowest terms, which would contradict our assumption that a and M have no factor in common.

In view of all this, we see that

$$E\left[s(x)\right] = \frac{1}{m}\sum_{x=0}^{M-1} s(x) = \frac{1}{m}\sum_{x=0}^{M-1} x = \frac{1}{2}(M-1) \tag{12}$$

and $$E\left[\{s(x)\}^2\right] = \frac{1}{M}\sum_{x=0}^{M-1}\{s(x)\}^2 = \frac{1}{M}\sum_{x=0}^{M-1} x^2 = \frac{1}{6}(M-1)(2M-1) \tag{13}$$

Now we only need to calculate

$$E\left[xs(x)\right] = \frac{1}{M}\sum_{x=0}^{M-1} xs(x) \tag{14}$$

We get this by following Knuth's method (Reference (4), pages 69-70). However, we have to correct a slight error in Knuth's equation (17), page 72, which is not valid for our case.

<u>Calculation of $E\left[xs(x)\right]$</u>

Following Knuth, we define the 'sawtooth' function

$$Z(z) = 0 \qquad \text{if } z \text{ is an integer} \tag{15}$$

$$Z(z) = z - \lfloor z\rfloor - \frac{1}{2} \qquad \text{if } z \text{ is not an integer} \tag{16}$$

where $\lfloor z \rfloor$ is the integral part of z. We also define the Dedekind sum

$$\sigma(h,k,0) = 12 \sum_{j=0}^{k-1} Z\left(\frac{j}{k}\right) Z\left(\frac{hj}{k}\right) \tag{17}$$

$$\text{so that } \sigma(a,M,0) = 12 \sum_{x=0}^{M-1} Z\left(\frac{x}{M}\right) Z\left(\frac{ax}{M}\right) \tag{18}$$

For any integer x in (1,M-1), we see from (16) that

$$\frac{x}{M} = Z\left(\frac{x}{M}\right) + \frac{1}{2} \tag{19}$$

Moreover from (1) and (16), for any integer x in (1,M-1) we have

$$\frac{s(x)}{M} \equiv \frac{ax}{M} \pmod 1 \tag{20}$$

$$\text{whence } \frac{s(x)}{M} = \frac{ax}{M} - \left\lfloor \frac{ax}{M} \right\rfloor = Z\left(\frac{ax}{M}\right) + \frac{1}{2} \tag{21}$$

Thus from (19) and (21), (14) becomes

$$E\left[xs(x)\right] = \frac{1}{M} \sum_{x=0}^{M-1} xs(x) = \frac{1}{M} \sum_{x=1}^{M-1} xs(x) = M \sum_{x=1}^{M-1} \left[Z\left(\frac{x}{M}\right) + \frac{1}{2}\right] \left[Z\left(\frac{ax}{M}\right) + \frac{1}{2}\right]$$

$$= M \sum_{x=1}^{M-1} Z\left(\frac{x}{M}\right) Z\left(\frac{ax}{M}\right) + \frac{1}{2} M \sum_{x=1}^{M-1} Z\left(\frac{x}{M}\right) + \frac{1}{2} M \sum_{x=1}^{M-1} Z\left(\frac{ax}{M}\right) + \frac{1}{4} M(M-1) \tag{22}$$

Now from (19)

$$\sum_{x=1}^{M-1} Z\left(\frac{x}{M}\right) = \sum_{x=1}^{M-1} \left(\frac{x}{M} - \frac{1}{2}\right) = 0 \tag{23}$$

and from (21) and (12)

$$\sum_{x=1}^{M-1} Z\left(\frac{ax}{M}\right) = \sum_{x=1}^{M-1} \left(\frac{s(x)}{M} - \frac{1}{2}\right) = \frac{1}{M} \sum_{x=1}^{M-1} s(x) - \frac{1}{2}(M-1) = \frac{1}{M} \sum_{x=1}^{M-1} x - \frac{1}{2}(M-1) = 0 \tag{24}$$

Hence, using (18), (23) and (24), we find that (22) gives

$$E\left[xs(x)\right] = \frac{M}{12}\ \sigma(a,M,0) + \frac{1}{4}\,M(M-1) \tag{25}$$

Calculation of C_1

We can now evaluate (7), using (8), (12) and (25), as

$$\mathrm{cov}\left[x,s(x)\right] = \frac{M}{12}\,\sigma(a,M,0) + \frac{1}{4}\,M(M-1) - \frac{1}{4}\,(M-1)^2$$

$$= -\frac{M}{12}\ \sigma(a,M,0) + \frac{1}{4}\,(M-1) \tag{26}$$

Similarly we can use (8), (9), (12) and (13) to show that

$$\mathrm{var}(x) = \mathrm{var}\left[s(x)\right] = \frac{1}{6}(M-1)(2M-1) - \frac{1}{4}(M-1)^2 = \frac{1}{12}\,(M^2-1) \tag{27}$$

From (26) and (27), (4) gives

$$C_1 = \frac{M\sigma(a,M,0)+3(M-1)}{M^2-1} \tag{28}$$

As already mentioned, this formula differs slightly from the formula in Knuth's book (Reference (4), page 72 equation (17)).

Calculation of $\sigma(a,M,0)$

On pages 72-74 of Reference (4), Knuth states and proves the reciprocity law for Dedekind sums, which in our case amounts to

$$\sigma(h,k,0) + \sigma(k,h,0) = \frac{k}{k} + \frac{k}{k} + \frac{1}{kh} - 3 \tag{29}$$

which hold provided that h and k have no common factors. In addition, Knuth recalls that

$$\sigma(h-nk,k,0) = \sigma(h,k,0) \text{ for any integer } n \tag{30}$$

and $$\sigma(-h,k,0) = -\sigma(h,k,0) \tag{31}$$

Since from (15) and (16) we see that $Z(z)$ is an odd function of z with period unity, the truth of (30) and (31) is fairly evident from the definition (17).

Another formula we will need is

$$\sigma(h,1,0) = \sigma(h,2,0) = 0 \qquad (32)$$

This is so because, when $j=0$ and $k=1$ or 2 in (17), the value of j/k is $0, \frac{1}{2}$ or 1, and for any of these values, (15) and (16) show that

$$Z\left(\frac{j}{k}\right) = 0 \qquad (33)$$

From (29), (30), (31) and (32) Knuth develops an algorithm for calculation $\sigma(h,k,0)$, based on the following steps:

(I) Reduce h by a multiple of k so that

$$\text{new } h = h^{1} = h - nk \text{ lies in } (-k/2, k, 2) \qquad (34)$$

$$\text{Set } \theta = \left.\begin{array}{ll} 1 & \text{if } h^{1} \geqslant 0 \\ -1 & \text{if } h^{1} < 0 \end{array}\right\} \qquad (35)$$

$$\text{and } h^{11} = |h^{1}| \qquad (36)$$

Then from (29), (30) and (31) we have

$$\sigma(h,k,0) = \sigma(h^{1},k,0) = \theta\,\sigma(h^{11},k,0)$$

$$= \left[\theta\ \frac{h^{11}}{k} + \frac{k}{h^{11}} + \frac{1}{h^{11}k} - 3 - \sigma(k,h^{11},0)\right] \qquad ..(37)$$

(II) <u>If $h^{11}=1$ or 2, stop</u>. Otherwise replace h by k, replace k by h^{11}, and return to Step I to evaluate the new $\sigma(h,k,0)$.

As you work through this algorithm, the arguments h and k get rapidly smaller. (The process is somewhat similar to Euclid's algorithm for finding a greatest common divisor.)

Computer programs were written, both for the HP 65 computer and for the IBM 360, to calculate $\sigma(a,M,0)$ by the above algorithm, and hence to calculate the serial correlation C_1 by means of (28). We had to be careful to carry sufficient digits to obtain correct results, particularly for the case of the IBM 360 generator. The HP 65, with its range of ten significant digits, was just about adequate. We had to use double precision with the IBM 360 program.

Serial Correlation Coefficients for Lags Other Than Unity

So far we have discussed the calculation of C_1, the serial correlation between a random number x and its immediate successor. We now discuss how to calculate the serial correlation C_s between a random number and the random number 's positions further on' in the sequence.

If a sequence of successive random numbers is denoted by $x_n, x_{n+1}, x_{n+2}, \ldots x_{n+s}$ we have, from (1),

$$x_{n+1} \equiv ax_n \pmod{M} \tag{38}$$

$$x_{n+2} \equiv ax_{n+1} \pmod{M} \tag{39}$$

and so on, up to

$$x_{n+s} \equiv ax_{n+s-1} \pmod{M} \tag{40}$$

It follows that x_{n+s} must be related to x_n by

$$x_{n+s} \equiv a^s x_n \pmod{M} \tag{41}$$

Moreover, if

$$a_s \equiv a^s \pmod{M} \tag{42}$$

we see that (41) is equivalent to

$$x_{n+s} \equiv a_s x_n \pmod{M} \tag{43}$$

In other words, the relation between x_{n+s} and x_n is similar to that between two successive random numbers x_{n+1} and x_n, except that the 'magic multiplier' a has to be replaced by a_s, given by (42).

Hence the formula for C_s, the serial correlation at lag s, will be identical with the formula for C_1, except that 'a' must be replaced by a_s. Hence, from (28),

$$C_s = \frac{M\sigma(a_s, M, 0) + 3(M-1)}{M^2 - 1} \tag{44}$$

Results of Calculations

The values of C_s, for s=1,2,3,...10, were calculated from equation (44), both for the IBM 360 and for the IBM 1130 versions of RANDU (with values of a and M as in equations (2) and (3)). The Dedekind sums in (44) were computed by the algorithm described at equations (34) to (37). The results are given in Tables I and II.

It will be seen that for both cases the lag correlations are extremely small up to s=10. For the IBM 360, Table I shows that all correlations are less than 0.000014. For the IBM 1130, Table II shows that all correlations are less than 0.00126.

Hence from the point of view of serial correlation, the behaviour of the random number sequences generated by RANDU seems extremely satisfactory.

We cannot understand why Stanford Univeristy rejected RANDU - but we have asked them to explain. For the moment, it looks as if it is reasonable to use RANDU in simulations in which the 'time series' behaviour of the random number sequence is important.

TABLE I

SERIAL CORRELATIONS FOR LAGS 1 TO 10 FOR THE IBM 360 VERSION OF RANDU WITH a = 65539 AND M = 2147483648

s	a_s	C_s
1	65539	1.4×10^{-5}
2	393225	2.3×10^{-6}
3	1769499	-4.5×10^{-6}
4	7077969	1.2×10^{-7}
5	26542323	-1.4×10^{-7}
6	95552217	2.1×10^{-8}
7	334432395	-3.4×10^{-8}
8	1146624417	-4.9×10^{-9}
9	1722371299	3.0×10^{-8}
10	14608041	1.3×10^{-7}

TABLE II

SERIAL CORRELATIONS FOR LAGS 1 TO 10 FOR THE IBM 1130 VERSION OF RANDU WITH a = 899 AND M = 32768

s	a_s	C_s
1	899	0.00126
2	21769	-0.00036
3	7835	-0.00032
4	31313	-0.00003
5	2675	0.00706
6	12761	-0.00040
7	3339	0.00057
8	19873	0.00044
9	7267	-0.00059
10	12201	0.00062

REFERENCES

(1) System/360 Scientific Subroutine Package (360A-CM-03X) Version III. Programmer's Manual. (Form H20-0305-3) page 77.

(2) 1130 Scientific Subroutine Package (1130-CM-02X). Programmer's Manual. (Form H20-0252-3) page 60.

(3) 'Datamation' July 1975, page 104.

(4) D.E. Knuth, 'The Art of Computer Programming', Vol. 2. (Addison-Wesley) 1969.

DISTRIBUTION

DLOR

DMOR

DAOR

D Log A

D Man A

ORAE Library -2

DSIS Library -2

DMS