電子計算機における擬似乱数の生成

真　田　克　彦

The Generation of Pseudo-Random Numbers on Computers

Katsuhiko SANADA

1. Introduction

An indispensable requirement of the Monte Carlo Method is a copious and reliable source of "uniformly distributed random numbers". More precisely, a facile method is needed for the generation of a sequence, called pseudo-random number, which strongly resembles a sample sequence drawn by repeated independent trials from a probability distribution uniform on the unit interval [0, 1]. Numbers generated by a formula cannot of course be random, but their use is almost a necessity in the computers now generally available. Ever since John Von Neumann introduced the "mid-square method" some twenty years ago, methods for the generation of such pseudo-uniform sequence in computer have received much attention.

Recently, the methods most widely accepted are the "mixed congruence method" proposed by R. R. Coveyou,

$$X_{n+1} \equiv AX_n + C \pmod{M}$$

and the "multiplicative congruence method" proposed by D. H. Lehmer,

$$X_{n+1} \equiv AX_n \pmod{M}$$

Here the modulus M generally equals one more than the largest (fixed point) integer which the computer can store, e.g. 2^m (for binary machines) or 10^m (for decimal machines; m is the word-length of the computer).

The sequence $\{X_n\}$ is the non-negative integers less than M. Finally, the sequence X_0/M, X_1/M, X_2/M, ...is taken to be the sequence of random numbers.

The hope is the parameters X_0, A, C and M have been chosen so that the resulting sequence appears to be drawn at random from the uniform distribution on [0, 1]. Length of period of the random sequence is one standard that has been used in the selection of parameters. Speed of generation is a second. But a great deal of freedom still remains, and the question of how best to use this freedom never has been fully answered.

If we had a complete understanding of relationship between the number theoretic properties of A, C and M, on the one hand, and the statistical properties of the sequence they generate, on the other hand, the selection problem essentially would be solved.

2. Mixed Congruence Method (1)

$$X_{n+1} \equiv AX_n + C \pmod{M} \qquad \text{.....(2-1)}$$

The multiplier A and the addend C are optional parameters of (2-1); both parameters are positive integers less than M and relatively prime to M.

The first problem is to choose X_0, A and C so that the period of the resulting sequence is as great as possible. This formula shows that the period of the sequence $\{X_n\}$ is not greater than M. When the period is short, the sequence comes to no good in randomness and too uniform. So it is to be desired that the period is as long as possible.

Next two theorems are ture. ([4], [8])

〔Theorem 2-1〕

If $A \equiv 1 \pmod 4$ and $C \equiv 1 \pmod 2$,

then the formula

$$X_{n+1} \equiv AX_n + C \pmod{2^m}$$

takes the longest period 2^m, on whichany initial value X_0 has no effect.

〔Theorem 2-2〕

If $A \equiv 1 \pmod{20}$ and $C \equiv 1, 3, 7$ or $9 \pmod{10}$,

then the formula

$$X_{n+1} \equiv AX_n + C \pmod{10^m}$$

takes the longest period 10^m, on which any initial value X_0 has no effect.

Theoretically these generators have a number of small advantages over the multiplicative generators. They can have longer periods, they may be used with any starting value, and on most machines, they can be faster than the fastest multiplicative generators. The fastest such generators have $A=2^p+1$ or $A=10^p+1$ for $p>1$, because these generators are easily effected by shift-and-add instructions in computer.

3. Mixed Congruence Method (2)

$$X_{n+1} \equiv AX_n + C \pmod{2^m} \qquad \text{.....(3-1)}$$

Here the parameter A is of the form (2^p+1) where p is an integer greater than 1; C may be any odd number, and m any positive integer. We start with any convenient X_0; the formula then generates all the integers from 0 to (2^m-1).

To illustrate the formula, suppose we take $p=2$, $m=3$, $X_0=0$, $C=1$. The formula then becomes

$$X_{n+1} \equiv 5X_n + 1 \pmod 8$$

whence $X_1=1$, $X_2=6$, $X_3=7$, $X_4=4$, $X_5=5$, $X_6=2$, $X_7=3$, $X_8=0$.

Now we make the proofs not to use number theory. ([2])

Consider the special case

$$X_{n+1} = AX_n + 1 \qquad \text{.....(3-2)}$$

with $X_0=0$, $A=2^p+1$, $p>1$ (integer)

By (3-2)

$$X_n=1+A+A^2+\cdots\cdots+A^{n-1}$$

If n is odd, X_n is odd. Because the X_n are alternately even and odd. .....(3-3)

If $n=2^L$, L any positive integer. Then X_n contains 2^L but not 2^{L+1}. .....(3-4)

By induction.

Assume it true for some L. Then

$$X_{2n}=1+A+\cdots\cdots+A_{n-1}+A^n(1+A+\cdots\cdots A^{n-1})$$
$$=(1+A^n)X_n$$

Here $1+A^n$ contains 2 exactly once. Because

$$\frac{1}{2}(A^n+1)=\frac{1}{2}\{(2^p+1)^n+1\}$$
$$=\frac{1}{2}\{(1+\text{terms in } 2^p)+1\}$$
$$=1+\text{terms in } 2^{n-1},\ \text{odd if } p>1$$

Then if X_n contains 2^L but not 2^{L+1}, X_{2n} contains 2^{L+1} but not 2^{L+2}.

But (3-4) is true if $L=1$, since $X_2=2^p+2$.

If $n=R\cdot 2^L$, where R is an odd number, then X_n contains 2^L but 2^{L+1}.....(3-5)

$$X_n=X_{R\cdot 2^L}=(1+A^R+A^{R\cdot 2}+\cdots\cdots+A^{R(2^L-1)})X_R$$
$$=(1+A^R)(1+A^{2R})(1+A^{2^2\cdot R})\cdots\cdots(1+A^{2^{L-1}\cdot R})X_R$$

X_n has exactly L factors of the form $(1+A^k)$; whence X_n contains 2^L but not 2^{L+1}, since X_R is odd.

Thus it follows from (3-3), (3-4) and (3-5) that if $0<n<2^Q$, X_n does not contain 2^Q. .....(3-6)

If Z_n is the remainder when X_n is divided by $s=2^m$, then the sequence Z_1, Z_2, Z_3,....., Z_{s-1} includes all the integers from 1 to $s-1$; that is, every possible remainder occurs exactly once. .....(3-7)

By (3-6), there is a remainder; i. e., $Z_i\neq 0$ if $1\leqq i<s$.

Assume $s>j>i$. If $Z_j=Z_i$, then X_j-X_i must contain s. But

$$X_j-X_i=A^i+A^{i+1}+\cdots\cdots+A^{j-1}$$
$$=A^i(1+A+\cdots\cdots+A^{j-i-1})$$
$$=A^iX_{j-i}$$

This cannot contain $s=2^m$, by (3-6).

Thus $Z_j\neq Z_i$ and no remainder occurs more than once. Since $(s-1)$ remainders occur, (3-7) is proved.

$$Z_i=Z_{i+s}$$

The Z_i form a periodic sequence with period 2^m. .....(3-8)

Because if $|i-j|$ contains 2^Q, so does $|Z_i-Z_j|$.

$$X_j-X_i=A^iX_{j-i}$$
$$=(h-k)2^m+(Z_j-Z_i)$$

where $X_j=Z_j+h\cdot 2^m$, $X_i=Z_i+k\cdot 2^m$

Let $H_i=\{X_n \mid \text{remainder is } Z_i \text{ when } X_n/2^m\}$

There are H_0, H_1, ..., H_{s-1} associated with Z_1, Z_2,....., Z_{s-1}.

Let $$X_{n+1}=AX_n+1 \qquad \text{.....(3-9)}$$
with $0<X_0<2^m$

By (3-7), X_0 is equal to some Z, say Z_k. Then

$$Z_k=X_0=1+A+.....+A^{k-1}-h\cdot 2^m$$
X_0 belongs to H_k.

$$X_1=1+A+.....+A^k-A\cdot h\cdot 2^m$$
X_1 belongs to H_{k+1}.

$$X_2=1+A+.....+A^{k+1}-A^2\cdot h\cdot 2^m$$
X_2 belongs to H_{k+2}.

and so on.

Thus, (3-7) remains true for arbitrary X_0.

Let $$X_{n+1}=AX_n+C$$
with $0<X_0<2^m$ and C any odd number. .....(3-10)

Then $$Z_k=X_0=C(1+A+A^2+.....+A^{k-1})-h\cdot 2^m$$
X_0 belongs to H_k.

$$X_1=C(1+A+A^2+.....+A^k)-A\cdot h\cdot 2^m$$
X_1 belongs to H_{k+1}.

and so on.

By the same proof with (3-7), it is shwon that no Z is repeated.

Thus we can state

[Theorem 3-1]

If $A=2^p+1$, $p>1$ (integer)

$0\leqq X_0<2^m$, $m>0$ (integer)

C=any odd number

then the formula (3-1) $X_{n+1}\equiv AX_n+C \pmod{2^m}$ generates a set of identical sequences of length 2^m, each containing all the integers 0 to 2^m-1.

4. Harmonics of Mixed Congruence Method

Since (3-1) generates all the integers from 0 to (2^m-1), it follows that for a sufficiently long sequence the mean and variance must agree exactly with the theoretical values for a uniformly distributed population. But it is shown that the sequence has not only the period 2^m, but also subperiods or harmonics of all lengths 2^i, $0<i<m$. These harmonics are subject to define patterns. ([2])

For example consider the series generated by

$$X_{n+1}\equiv 9X_n+13 \pmod{32}$$

$X_0=0$, $X_1=13$, $X_2=2$, $X_3=31$, $X_4=4$, $X_5=17$, $X_6=6$, $X_7=3$,

$X_8=8$, $X_9=21$, $X_{10}=10$, $X_{11}=7$, $X_{12}=12$, $X_{13}=25$, $X_{14}=14$, $X_{15}=11$,

$X_{16}=16$, $X_{17}=29$, $X_{18}=18$, $X_{19}=15$, $X_{20}=20$, $X_{21}=1$, $X_{22}=22$, $X_{23}=19$,
$X_{24}=24$, $X_{25}=5$, $X_{26}=26$, $X_{27}=23$, $X_{28}=28$, $X_{29}=9$, $X_{30}=30$, $X_{31}=27$,
$X_{32}=0$, $X_{33}=13$, ...

By upper table, we know that $|X_{n+16}-X_n|=16$. Whatever the length of the period, $|X_{n+2^{m-1}}-X_n|=2^{m-1}$

If we consider quarter-periods, $|X_{n+2^{m-2}}-X_n|$ is always a multiple of 2^{m-2}.

This relationship holds whatever the values of p and C; it is an inherent property of (3-1).

If $X_0=0$ and $X_{n+1}=AX_n+C$, then

$$X_{n+2k}-2X_{n+k}+X_n=(A^k-1)\cdot A^n\cdot C/(A-1)$$

Since $A=2^p+1$,

$$(A^k-1)/(A-1)=k^2 2^p+(\text{terms in higher powers of } 2^p)$$

If $k=2^Q$, $2Q\geqq m-p$, then

$$X_{n+2k}-2X_{n+k}+X_n\equiv 0 \pmod{2^m}$$

Thus three equally spaced X_n, X_{n+k}, and X_{n+2k} of the sequence $\{X_n\}$ are in arithmetic progression modulus 2^m. So also if k is a multiple of 2^Q.

If $k=2^Q$, $2\cdot Q\geqq m-p$, then

$$X_{n+k}-X_n\equiv \text{const.} \pmod{2^m}$$

And if $2\cdot Q\geqq m-p-1$, then

$$X_{n+3k}-X_{n+2k}\equiv X_{n+k}-X_n \pmod{2^m}$$

We can state the same for decimal system.

Thus we know that p should be kept small. Aside from reducing computer time, small values of p increase the length of the cycle for arithmetic progression.

5. Statistical Properties

We consider serial correlation $\rho(X_n, X_{n+1})$ between the consecutive random numbers X_n and X_{n+1} generated by (2-1). ([1])

Let A and C of (2-1) be values for which the period of the $\{X_n\}$ sequence is M and the sequence contains all integers from 0 to $M-1$ (chaotically disordered), with each integer appearing exactly once.

$$\rho(X_n, X_{n+1})=\frac{E(X_n, X_{n+1})-\{E(X_n)\}^2}{E(X_n^2)-\{E(X_n)\}^2} \qquad \text{.....(5-1)}$$

where $E(X_n)=(M-1)/2$ $\qquad E(X_n^2)=(M-1)(2M-1)/6$

Let $AX_n+C=q_n\cdot M+r_n$ $\qquad$ .....(5-2)

with $0\leqq q_n,\ r_n<M$

$$E(X_n, X_{n+1})=(1/M)\sum_{X=0}^{M-1} X_n\cdot X_{n+1}$$
$$=(1/M)\sum_{X=0}^{M-1} X(AX+C-qM)$$
$$=A\cdot E(X^2)-CE(X)-\sum_{X=0}^{M-1} qX \qquad \text{.....(5-3)}$$

(Dispensing with the subscript n for convenience)

Assume for the moment that $C \geqq A$ and let X_n in (5-2) take on consecutive integer values starting with 0. Then q increases from 0 to A, in increments of 1, and each q has associated with $[M/A]$ or $[M/A]+1$ 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 $\bar{r}_0=C$, and for $q \geqq 1$, $\bar{r}_q < A$ is given by

$$\bar{r}_q = C - qM \pmod{A} \quad \bar{r}_q < A \qquad \text{.....(5-4)}$$

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

$X=(qM+\bar{r}_q-C)/A$ corresponding to $\bar{r}_q$ and

$X=\{(q+1)M+\bar{r}_{q+1}-C\}/A$ to $\bar{r}_{q+1}$, whence

$(qM+\bar{r}_q-C)/A \leqq X < \{(q+1)M+\bar{r}_{q+1}-C\}/A$ corresponding to q.

Hence

$$\sum_{X=0}^{M-1} Xq = \frac{AM^2}{3} - \frac{AM}{4} - \frac{C^2}{2A} + \frac{M}{4} - \frac{C}{2A} + \frac{CM}{2A} + \frac{A}{12} + \frac{CM}{2} - \frac{1}{12A} - \frac{M^2}{4} - \frac{M^2}{12A} - \frac{MS}{A^2} \quad \text{...(5-6)}$$

where $$S=\sum_{q=1}^{A} \bar{r}_q \cdot q \qquad \text{.....(5-6)}$$

We make the assumption that M is so large that any term order of magnitude is $1/M$ or less is negligible.

$$\rho(X_n, X_{n+1}) \fallingdotseq \frac{1}{A} - \frac{6C}{AM}\left(1-\frac{C}{M}\right) + \frac{12}{M}\left(\frac{S}{A^2}-\frac{A}{4}\right) \qquad \text{.....(5-7)}$$

$$\left|\frac{12}{M}\left(\frac{S}{A^2}-\frac{A}{4}\right)\right| \leqq \frac{A}{M}$$

When $A/M \ll 1/A$, the third term is negligible. But for A on the order of $M^{\frac{1}{2}}$ or larger, the third term may predominate and the complete equation (5-7) must be used.

For the case $C<A$,

$$\rho(X_n, X_{n+1}) \fallingdotseq \frac{1}{A} + \frac{12}{M}\left(\frac{S}{A^2}-\frac{A}{4}\right) \qquad \text{.....(5-8)}$$

where $$S=\sum_{q=1}^{A-1} \bar{r}_q \cdot q \qquad \text{.....(5-9)}$$

The two definitions (5-6) and (5-9) cannot give results for ρ different by more than negligible amount. So equation (5-8) shows that equation (5-7) still applies for the case of $C<A$. For this case, however, the middle term of (5-7) is insignificant and the parameter C appears only insofar as it influences the value of S.

[Example 5-1]

Suppose that $M=2^{35}$, $A=2^{34}+1$ and $C=1$.

Equation (5-7) reduces to

$$\rho(X_n, X_{n+1}) \fallingdotseq \frac{1}{4}$$

which agrees with the result given earlier.

〔Example 5-2〕

Suppose that $M=2^{35}$, $A=2^{18}+1$, and $C=1$.

$$\rho(X_n,\ X_{n+1})\fallingdotseq 2^{-18}-2^{-18}$$

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

In some respects the best choice of A is approximately $M^{\frac{1}{2}}$. One reason is that this choice ensures an absolute value of ρ on the order of $M^{-\frac{1}{2}}$, irrespective of C. For many C, $|\rho|$ may be much smaller. Example 5-2 shows this fact. But it is not correct to conclude that this selection of parameters produces an acceptable generator. For one thing, the first several hundred numbers generated by this combination, starting with $X_0=0$, are all less than $M/2$.

〔Example 5-3〕

Suppose that $M=2^{35}$ and $A=2^{17}+1$.

$$\rho(X_n,\ X_{n+1})\fallingdotseq 3(C^2\cdot 2^{-67}-C\cdot 2^{-32}+1)2^{-19}$$

Thus when $C=1$, $\rho\fallingdotseq 3(2^{-19})$; and when $C\fallingdotseq(1\pm 2^{-\frac{1}{2}})2^{34}$ and approximately divisible by A, $\rho\ll 2^{-19}$.

Finally, if A is sufficiently small relative to $M^{\frac{1}{2}}$ so that $A/M\ll 1/A$, then

$$\rho(X_n,\ X_{n+1})\fallingdotseq\frac{1}{A}\left(\frac{6C^2}{M^2}-\frac{6C}{M}+1\right)$$

It follows that $\rho\fallingdotseq 1/A$ when $C\ll M$, whereas $\rho\ll 1/A$ when $C\fallingdotseq M(1\pm 3^{-\frac{1}{2}})/2$. Here A and C are restricted to values which afford the full period. One such selection of $M=2^{35}$, namely $A=2^7+1$ and $C=1$, has been tested empirically and proposed as a suitable generator. ([9])

References

1) Martin Greenberger, "An A Priori Determination of Serial Correlation in Computer Generated Random Numbers", Math. Comp. 15 (1961)
2) Paul Peach, "Bias in Pseudo-Random Numbers," J. Amer. Statist. Assoc. 56 (1961)
3) J. L. Allard, A. Dobell and T. E. Hull, "Mixed Congruential Random Number Generators for Decimal Machines," Journal of the ACM, 10, No. 2 (1963)
4) Masaaki Shibuya, "Generation of Pseudo Random Number," in Japanese, Sugaku 15, No. 2 (1963)
5) Yu. A. Shreider, "The Monte Carlo Method," Pergamon Press
6) Martin Greenberger, "Notes on a New Pseudo-Random Number Generator," Journal of the ACM 8(1961)
7) R.R. Coveyou and R. P. Macpherson, "Fourier Analysis of Uniform Random Number Generators," Journal of the ACM 14, No. 1 (1967)
8) Takao Tsuda, "Monte Carlo Method and Simulation," in Japanese, Baihukan, Tokyo
9) A. Rotenberg, "A New Pseudo-Random Number Generator," Journal of the ACM 7 (1960)
10) Samuel Gorenstein, "Testing a Random Number Generator, Comm. of the ACM 10, No. 2 (1967)