RANDOM NUMBERS

4.1 Random Numbers

The earlier chapters have very clearly illustrated that random numbers are a necessary basic ingredient in the application of Monte Carlo method or simulation of situations involving randomness. There are a large number of systems, where chance plays a part. These systems are called *stochastic* systems. Even for the solution of problems, which are deterministic, random numbers are required for simulation.

What are random numbers? These numbers are samples drawn from a uniformly distributed random variable between some specified intervals, and they have equal probability of occurrence.

Properties of Random Numbers :

A sequence of random numbers has two important statistical properties.

- uniformity, and
- independence.

Each random number is an independent sample drawn from a continuous uniform distribution between an interval 0 to 1. The probability density function (pdf) is shown in Fig. 4.1 and is given by,

$$f(x) = \begin{cases} 1, 0 \le x \le 1 \\ 0, \textit{otherwise} \end{cases}$$

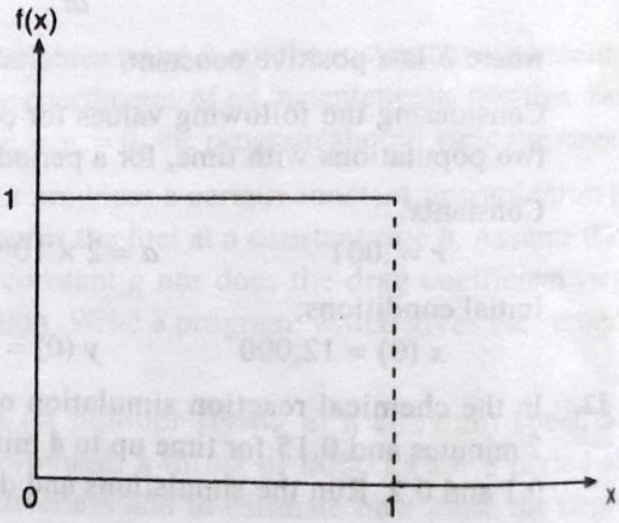

Fig. 4.1

The expected value of each random number R_i is given by

$$E(R) = \int_0^1 x\,dx = \frac{x^2}{2}\Big|_0^1 = \frac{1}{2}$$

and variance is given by $V(R) = \int_0^1 x^2\,dx - [E(R)]^2 = \frac{x^3}{3}\Big|_0^1 - \left[\frac{1}{2}\right]^2 = \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$

If the interval between 0 and 1 is divided into n equal parts or classes of equal length, then,

- the probability of observing a value in a specified interval is independent of the previous values drawn.
- if a total of m observations are taken, then the expected number of observations in each interval is m/n, for uniform distribution.

4.2 Random Number Table

Let us conduct a simple experiment to demonstrate the generation of random numbers. Take ten identical chips of paper and write down the digits 0, 1, 2, 3, ..., 9 on them. Put them in a box, mix them well, and take out one chip. It is a random number between 0 and 9 both inclusive. Repeat this

experiment, each time returning the chip to the box and mixing them well. Instead of 10 pieces of paper we can have say 50 with digits 0, 1, 2, 3, ..., 9 repeated 5 times. Each time, draw 5 pieces and note down their numbers. Thus each time 5 random digits are obtained. These can be listed in the form of a table similar to Appendix Table A-1. Such a table is called a random number table. The most comprehensive of all published tables of random numbers is due to RAND Corporation, which contains one million random digits. These numbers were generated by using a special roulette, which incorporated electric devices. A simple roulette wheel, shown in Fig. 4.2, comprises of a disc divided into 10 equal sectors numbered from 0 to 9. The rotating disc is abruptly stopped and the number against the pointer is noted down as a random digit.

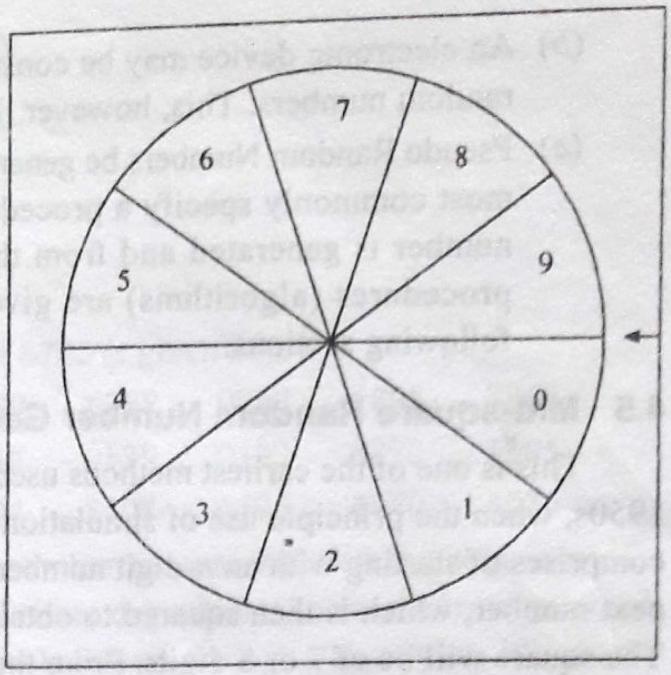

Fig. 4.2

4.3 Pseudo Random Numbers

The 'pseudo' means false. But here word 'pseudo' implies that the random numbers are generated by using some known arithmetic operation. Since, the arithmetic operation is known and the sequence of random numbers can be repeatedly obtained, the numbers cannot be called truly random. However, the pseudo random numbers generated by many computer routines, very closely fulfill the requirement of desired randomness.

If the method of random number generation that is the random number generator is defective, the generated pseudo random numbers may have following departures from ideal randomness.

- The generated numbers may not be uniformly distributed.
- The generated numbers may not be continuous.
- The mean of the generated numbers may be too high or too low.
- The variance may be too high or too low.
- There may be cyclic patterns in the generated numbers, like;
  - (*a*) Auto correction between numbers.
  - (*b*) A group of numbers continuously above the mean, followed by a group continuously below the mean.

Thus, before employing a pseudo random number generator, it should be properly validated, by testing the generated random numbers for randomness. The random number tests commonly used are explained in Sections 4.10 to 4.14.

4.5 Mid-square Random Number Generator

This is one of the earliest methods used for generating pseudo random numbers. It was used in 1950s, when the principle use of simulation was in designing thermonuclear weapons. The method comprises of starting with an *n*-digit number, squaring it and taking the *n* digits in the middle as the next number, which is then squared to obtain the next number. Say, we start with a 4-digit number. The square will be of 7 or 8 digits. From the squared number chop off the two low order digits and one or two high order digits, to obtain a 4-digit number in the middle.

Let the *seed* number be 5673, when squared we get 32182929. After removing two low order digits and two high order digits, we get the next random number 1829. Its square is 3345241. After removing two low order and one high order digit, we get 3452 as random number. Some random numbers obtained from the seed 5673 are;

5673	1829	3452	9163	9605	2560	5536
6472	8867	6236	8876	7833	3558	6593
4676	8649	8052	8347	6724	2121	4986
8601	9772	4919	1965	8612	1665	7722
6292	5892	7156	2083	3388	4785	8962

A computer program in C language for generating random numbers by the mid-square algorithm

4.6 Congruence Method or Residue Method

The most commonly employed pseudo random number generators use the congruence method, also called the method of power residues. This algorithm is described by the expression,

$$r_{i+1} = (ar_i + b) \text{ modulo } m$$

Where a, b and m are constants, r_i and r_{i+1} are ith and $(i + 1)$th random numbers. The expression implies multiplication of a by r_i addition of b and then dividing by m. The r_{i+1} is the remainder or residue. To begin the process of random number generation, in addition to a, b and m, the value of r_0 is also required. It may be any random number and is called **seed.**

The congruential random number generator may be of the additive, multiplicative or mixed type. The expression given above with $a > 1$ and $b > 0$ is of the mixed type.

If $a = 1$, the expression reduces to the *additive* type.

$$r_{i+1} = (r_i + b) \text{ modulo } m$$

If $b = 0$, the expression reduces to the multiplicative congruential method.

$$r_{i+1} = ar_i \text{ modulo } m.$$

The multiplicative methods are considered better than the additive methods and are as good as the mixed methods.

The selection of values for the constants a, b and m is very important, because on them depends the length of the sequence of random numbers, after which the sequence repeats. It is not possible to generate a non-repeating sequence of numbers with these methods. However, a sufficiently long sequence can be obtained by making a suitable selection of the constants. Since the number can be predicted, rather computed from r_i, and the whole string is reproducible, the numbers obtained are not truly random. They are called pseudo random numbers and hence the method is termed as pseudo random number generator.

Most of the computer languages have a standard function for generating random numbers.

In the modern scientific calculators, a random number key is provided. While pressed a random number between 0.000 and 0.999 is generated.

Example 4.1. The pseudo random number generation by the congruential methods can be illustrated by taking some values for a, b and m in the recursive equation.

$$r_{i+1} = (ar_i + b) \bmod m$$

It is better to start with a prime number as modulus m, and prime multiplier a; b can be taken any, say 1. The seed r_0 may be any.

...y, say 1. The seed r_0 may be any.

(a) Mixed Multiplicative Congruential (MMC) Generator :

Taking $a = 13$, $b = 1$ and $m = 19$

And let $r_0 = 1$

$r_1 = (1 \times 13 + 1) \mod 19 = 14 \mod 19 = 0$ residue $14 = 14$

$r_2 = (14 \times 13 + 1) \mod 19 = 183 \mod 19 = 9$ residue $12 = 12$

$r_3 = (12 \times 13 + 1) \mod 19 = 157 \mod 19 = 8$ residue $5 = 5$

$r_4 = (5 \times 13 + 1) \mod 19 = 66 \mod 19 = 3$ residue $9 = 9$

$r_5 = (9 \times 13 + 1) \mod 19 = 118 \mod 19 = 6$ residue $4 = 4$

$r_6 = (4 \times 13 + 1) \mod 19 = 53 \mod 19 = 2$ residue $15 = 15$

$r_7 = (15 \times 13 + 1) \mod 19 = 196 \mod 19 = 10$ residue $6 = 6$

$r_8 = (6 \times 13 + 1) \mod 19 = 79 \mod 19 = 4$ residue $3 = 3$

$r_9 = (3 \times 13 + 1) \mod 19 = 40 \mod 19 = 2$ residue $2 = 2$

$r_{10} = (2 \times 13 + 1) \mod 19 = 27 \mod 19 = 1$ residue $8 = 8$

$r_{11} = (8 \times 13 + 1) \mod 19 = 105 \mod 19 = 5$ residue $10 = 10$

$r_{12} = (10 \times 13 + 1) \mod 19 = 131 \mod 19 = 6$ residue $17 = 17$

Random numbers between 0 and 1 can be generated by

$$R_i = \frac{r_i}{m}, \; i = 1, 2, 3, \ldots\ldots$$

which gives the sequence as,

$$R_1 = \frac{14}{19} = 0.7368 \qquad R_2 = \frac{12}{19} = 0.6316 \qquad R_3 = \frac{5}{19} = 0.2632$$

$$R_4 = \frac{9}{19} = 0.4737 \qquad R_5 = \frac{4}{19} = 0.2105 \qquad R_6 = \frac{15}{19} = 0.7895$$

$$R_7 = \frac{6}{19} = 0.3158 \qquad \text{etc} \ldots\ldots$$

(*b*) Multiplicative Congruential (MC) Generator :

$$r_{i+1} = ar_i \bmod m$$

Again taking $a = 13$, $m = 19$, and seed $r_0 = 1$

$$r_1 = 1 \times 13 \bmod 19 = 0 \quad \text{residue } 13 = 13$$
$$r_2 = 13 \times 13 \bmod 19 = 8 \quad \text{residue } 18 = 18$$
$$r_3 = 13 \times 18 \bmod 19 = 12 \quad \text{residue } 6 = 6$$
$$r_4 = 13 \times 6 \bmod 19 = 4 \quad \text{residue } 2 = 2$$
$$r_5 = 13 \times 2 \bmod 19 = 1 \quad \text{residue } 7 = 7$$
$$r_6 = 13 \times 7 \bmod 19 = 4 \quad \text{residue } 15 = 15$$
$$r_7 = 13 \times 15 \bmod 19 = 10 \quad \text{residue } 5 = 5$$
$$r_8 = 13 \times 5 \bmod 19 = 3 \quad \text{residue } 8 = 8$$
$$r_9 = 13 \times 8 \bmod 19 = 5 \quad \text{residue } 9 = 9$$
$$r_{10} = 13 \times 9 \bmod 19 = 6 \quad \text{residue } 3 = 3$$
$$r_{11} = 13 \times 3 \bmod 19 = 2 \quad \text{residue } 1 = 1$$

The sequence of numbers obtained is 1, 13, 18, 6, 2, 7, 15, ...

(c) Additive Congruential Generator :

$$r_{i+1} = (r_i + b) \bmod m$$

Again taking $m = 19$ and $b = 11$

Taking seed $r_0 = 1$

$$r_1 = (1 + 11) \bmod 19 = 12$$
$$r_2 = (12 + 11) \bmod 19 = 4$$
$$r_3 = (4 + 11) \bmod 19 = 15$$
$$r_4 = (15 + 11) \bmod 19 = 7$$
$$r_5 = (7 + 11) \bmod 19 = 18$$
$$r_6 = (18 + 11) \bmod 19 = 10$$
$$r_7 = (10 + 11) \bmod 19 = 2$$
$$r_8 = (2 + 11) \bmod 19 = 13$$
$$r_9 = (13 + 11) \bmod 19 = 5$$
$$r_{10} = (5 + 11) \bmod 19 = 16$$
$$r_{11} = (16 + 11) \bmod 19 = 8$$
$$r_{12} = (8 + 11) \bmod 19 = 1$$

4.7 Arithmetic Congruential Generator

Another kind of pseudo random number generator is the arithmetic congruential algorithm, which is given as,

$$r_{i+1} = (r_{i-1} + r_i) \bmod m$$

The process starts with two random numbers, which are added and divided by m with the residue giving the third number. Then 2nd and 3rd numbers result into 4th number, and so on.

Random

For example,

If $r_1 = 9$, $r_2 = 13$ and $m = 17$

$r_3 = (9 + 13) \bmod 17 = 5$

$r_4 = (13 + 5) \bmod 17 = 1$

$r_5 = (5 + 1) \bmod 17 = 6$

$r_6 = (1 + 6) \bmod 17 = 7$

$r_7 = (6 + 7) \bmod 17 = 13$

$r_8 = (7 + 13) \bmod 17 = 3$

$r_9 = (13 + 3) \bmod 17 = 16$

$r_{10} = (3 + 16) \bmod 17 = 2$

nd so on as 1, 3, 4, 7, 11, 13, 8, 4, 12, 16, 11, 10, 4, 14, 1, 15, 16, 14, 13, 10, 6, ...

This results into quite a long sequence.