Random Numbers

Mark Anthony Caruana

Abstract

It is very difficult to define 'randomness'. However a simple definition of Random Numbers would be as follows: Random numbers can be defined as a sequence of numbers which do not follow a regular pattern. Thus one cannot possibly guess the value of the next number in the sequence, as this may be bigger, equal or smaller than its previous values or set of values. An example of a random number sequence is: 1, 7, 13, 24, 8, 3, 6, 50, 39, 86, 87, 2, ...
We describe how random sequences may be generated, and tested for randomness.

How to generate such sequences

The use of physical devices

Some examples are:
Counting the number of telephone calls received each day.
Counting radioactive particles for some time.

Various problems are encountered in such processes. They are time consuming and expensive. It is impossible to re-create the sequence and the 'randomness' of the source is questionable.

The use of irrational numbers

Today scientists have managed to come up with millions of digits after the decimal point of the irrational number π.

$$\pi = 3.141592654...$$

One can therefore use these numbers (the numbers found after the decimal point) as random numbers. The problems however are that: huge memory is needed, little is known about the distribution of such numbers and the process is time consuming.

Using Pseudorandom Generators

These are algorithms that produce perfectly deterministic predictable periodical sequences of numbers which nonetheless look and behave as if they where completely random.

Mid-Square Method

This algorithm was suggested by John von Neumann and is based on the following algorithm:

1. start with a certain seed
2. square it
3. take the middle digits
4. repeat the procedure

Some examples are:
Example 1:
Let $X_0 = 4444$(the seed)
$(X_0)^2 = 19749136$
$X_1 = 7491$ (taking the middle digits)
$(X_1)^2 = 56115081$
$X_2 = 1150$
$(X_2)^2 = 0132250$
$X_3 = 3225$

4444,7491,1150.3225,... (One can obviously divide the 10000 in order to obtain values between 0 and 1)

Example 2:
Let $Y_0 = 1000$
$(Y_0)^2 = 1000000$
$Y_1 = 0000$
$(Y_1)^2 = 0000$
etc...

As can be seen from the above, the method fails if the middle values are zero since the rest of the sequence would be composed entirely of zeroes.

Linear Congruential Generators(LCG)

These generators where introduced by Lehmer in 1948, and the values are computed by the following formula:

$$X_i = (aX_{i-1} + c) \ mod \ m$$

where a = multiplier c = adder
X_0 = seed $X_i = i^{th}$ value
m = modulus

In short, the above can be written in the following way: LCG(m,a,c,x_0)
Example: LCG(2^5,5,0,13)

$$X_1 = (5\times13 + 0\ ) \bmod 32$$
$$X_1 = 65 \bmod 32$$
$$X_1 = 1$$
$$X_2 = (5\times1 + 0) \bmod 32$$
$$X_2 = 5$$
$$X_3 = (5\times5 + 0) \bmod 32$$
$$X_3 = 25$$
$$13,1,5,25\ldots$$

Tests on Sequences of Random Numbers

1. Hamming Test

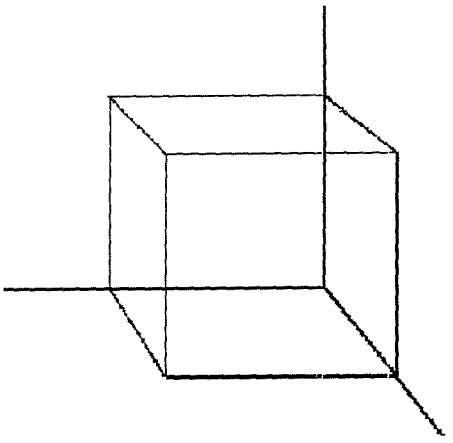
Checks whether some numbers appear more frequently than others, in a sequence of generated numbers.

2. Spectral Tests

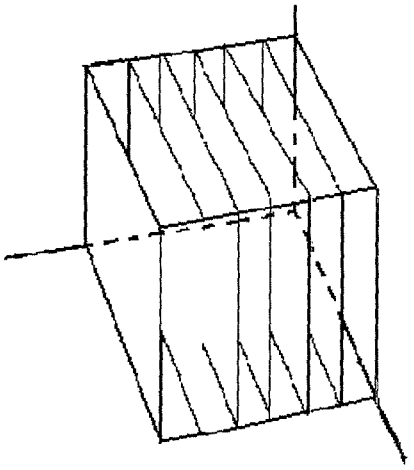
These methods are based on the fact that n-tuples of random numbers are always located in n-dimensional hyperplanes. If the distance between the planes is large, then the generator would have failed the test. Let us consider the following sequence of random numbers (evenly distributed
in the range (0,1)): 0.9501,0.2311,0.6068,0.4860,0.8913,0.7621,0.8214,0.4447,0.6154,0.7919,... Now if the generated numbers had to be evenly placed in cells, each cell containing three numbers of the sequence i.e.

(0.95,0.23,0.61)
(0.49,0.89,0.76)
etc

and later plotted on the xyz-axes, one should expect that these points would be evenly distributed in a unit cube (the shaded region) i.e.



In reality however they will more likely be placed in a series of parallel planes within the unit cube:



the smaller the distance between the planes the better the generator.
Random numbers are an important tool in a broad range of scientific research and have become indispensible in computer science.