

Counting On Chance

Computers are completely rational, which makes them superior to humans for many tasks. Choosing a random number, however, is an irrational task, and therefore impossible for a computer

'Pick a number at random'. This is one of the easiest things for a person to do but, paradoxically, for a computer this simple task is impossible.

A random number is a number that is impossible under any circumstances to predict. A computer simply follows instructions and needs a reason for every action it takes, so any number it creates will be a consequence of a series of instructions. No matter how complicated these instructions are, the number is still theoretically predictable — to find it you just follow the instructions that the computer did — and so the number is not truly random.

Truly random numbers can, however, be obtained from physical processes. For example ERNIE (Electronic Random Number Indicator Equipment) uses the random motion of free electrons to pick the winners of premium bonds.

It was von Neumann who hit upon the idea of pseudo-random numbers — numbers that could be created mathematically. His method was to take a four-digit number, say 4321, and square it. From the resulting eight-digit answer, 18671041, he took the central four digits, 6710, as the random number. This then becomes the 'seed' for the next number to be created. So 6710 squared gives 45024100, the central digits of which are 0241, giving the next random number, and so on. This squaring process can continue indefinitely but since the total of possible different numbers with four digits is limited (9999) sooner or later the sequence must begin to repeat itself.

Modern computers use more involved methods that give better pseudo-random numbers. For example, the BBC Micro can generate a random number approximately every 1.5 milliseconds, and if the computer were generating these numbers continuously the sequence would take 150 days before it began to repeat itself.

Random numbers were first generated



The Monte Carlo Method

This method was invented by John von Neumann and uses random numbers to calculate the answers to mathematical problems. In mathematics you often need to calculate the area bounded by a curve and this in a way is analogous to finding the area of an island when you have only a map of the coastline. The map of Britain is shown in a box of a known size that is to be bombarded by random points. Since the positions of the points are randomly generated they will fall over the total boxed area and the number that falls within the landmass is proportional to the land area of Britain. Using 40 random points we found 24 fell at sea and 16 on the land. Hence the area of the land is:

$$16/40 \times (1050 \times 550) = 16/40 \times 577,500 = 231,000 \text{ sq km.}$$

Using a greater number of random points would result in a closer approximation to the true figure of 229,523 square kilometres

electronically for use by telephone engineers trying to simulate fluctuations in demand on exchanges. Today there are many uses, from computer games to simulation of randomly fluctuating processes, to evaluating difficult mathematical functions. For most purposes, modern algorithms for pseudo-random numbers can be considered truly random.

The Rational Ass

Imagine you put a totally rational donkey midway between two identical piles of hay. The donkey cannot choose the larger pile because the two piles are identical, and it cannot choose the nearer one because it is exactly midway between the two. So perhaps it goes to the one it glances at first. But why does it glance at one rather than the other? Since there is no reason to choose one pile rather than the other, the donkey just stands there and starves to death. Similarly, computers cannot generate truly random numbers, because they do everything strictly according to reason

