

The randomness of randomness

S. Parthasarathy
drpartha@gmail.com

By just looking at the tracks, you can't say which way the train went (or which way will it come from)

..... Anon.

It all started with a rather innocent looking question on the Internet. ¹ Here is how it ran: Given a number (only one), we can answer certain questions about it e.g. is it a prime ? is it an even number ? etc. Now, given a number (only one) can we say if it is a random number ? Why not ?

I posted the above question on the Internet, and got some replies, all of which gave rise to more questions.

Some of the responders were statisticians in the traditional sense. And predictably, they took examples of their pet random process: tossing a coin, or casting a die. Yes, given no other information, such experiments may be considered to give random outcomes (will it be a head ? will be a tail ? will the die yield an even number ? will the next child be a boy ? ...). But, there is a catch somewhere deep within this premise. A physicist friend of mine argued that there could be no such thing as a random number generated by such devices (die, coin). After all, the outcome of a toss is bound by strict laws of physics. It is a different thing that we cannot measure exactly the various parameters influencing the outcome e.g. the force exerted by the thumb when tossing a coin, the velocity of air, temperature gradients, ballistics etc. All of these are important, to determine the exact trajectory of the coin, and hence the exact outcome of this experiment. If we could measure (and control) all these, there will be no such thing as a random toss (idem for a die). We can put forth such arguments for all such

¹This article is accessible on the w-w-web at :
<http://drpartha.org.in/publications/randomness.pdf>

so-called random phenomena when they involve physical devices and objects.

We will stop tossing coins in the air, or throwing dice on the table, and look for some non-physical phenomenon, for generating random numbers. Let us look at the last digit of the first n (assume $n=20$ for this case) prime numbers [1]. Here's what we get: 2 3 5 7 1 3 7 9 3 9 1 7 1 3 7 3 9 1 7 1 ? Looks like a perfect chain of random numbers (perhaps generated by a ten-faced die). Can you predict what would be the 21st number in this sequence (marked by a ?) ? NO. Wrong again – we can predict exactly the 21st digit which follows the last one above: 3, if we know the secret potion which created that sequence (the 21st prime is 73) .

Look at this, from another viewpoint. Suppose, we decide to write these random numbers in a binary notation. And now, we look at the last digit only (in this case we must call it a bit). Here's what we will get: 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 ad infinitum. Nothing could be more predictable than this series !

Now, let us look at the first n ($n=20$) primes themselves: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71.... ??

If we know the magic potion which was used for generating the above numbers, then we can predict exactly the number which must follow (the 21st prime number) 73. 73 is a predictable number (non random) now.

If we ignore for a moment the monotonically increasing magnitudes, and if we hide the common phenomenon behind these numbers (the fact that they are all primes), we probably have a good candidate for random numbers. Suddenly, the same 21st number becomes random and unpredictable !

Compare this with the following scenario : Imagine standing (in a safe spot) on a busy highway. Try to record the registration number of every car that passes by. Create a sequence, like earlier, of the last digit of each number plate. Can you predict the next digit in the sequence ? NO, because you know nothing about the cars which will drive your way.

The conclusion is simple, there is no such thing as a true random number (when taken all alone) ! It is just whether we are or we are not able to formalise the underlying generating phenomenon that makes all the difference. Some people prefer to use a more explicit term: non-deterministic phenomenon, to refer to such processes.

This topic is of such fundamental importance that Knuth [2] devotes a whole Section of his book to “random sequences” and quotes D.H. Lehmer (1951) explicitly *A random sequence is a vague notion embodying an idea of a sequence in which each term is unpredictable to the uninitiated...*

In fact, Knuth [2] carries this idea a bit further, by paraphrasing George Marsaglia *If the numbers are not random, they are at least higgledy-piggledy*

Let us go back and look at the question which started all this. The answer is a big NO. Can someone explain why ? Send your replies and remarks to the author, by email (drpartha@gmail.com).

References

- [1] The first 1000 primes, URL: <http://www.utm.edu/research/primes>
- [2] D. E. Knuth, What is a random sequence ?, The art of computer programming, Vol. 2, Seminumerical algorithms, Chapter 3.5, Pub.: Pearson Education Inc. Delhi, India.
