Sketches of a Lecture on Random Numbers

Davar Khoshnevisan*

July 3, 2004

Abstract

This note describes the essence of a lecture that was delivered on the 28th of June, 2004 at the University of Utah. It is recorded for possible future use.

1 Randomness is Everywhere!

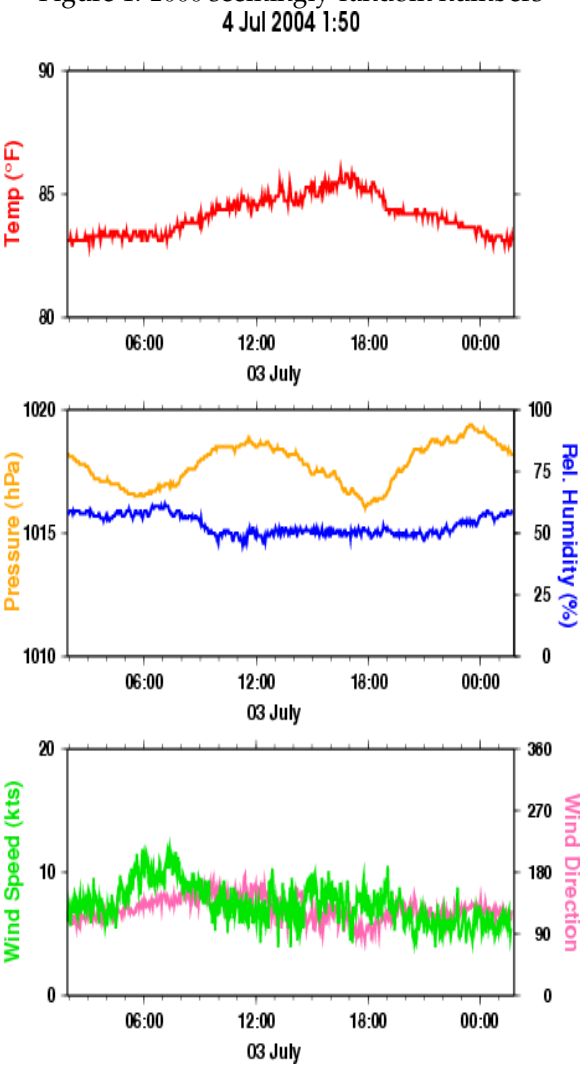
Despite the crude apostrophe, this section title is not an exaggeration. To further this point of view, a few minutes ago (11:58 p.m. Mountain time), as I was typing this document I looked at the RSMAS weather database on the web (`http://www.rsmas.miami.edu/enviroNewtonent/wx/`) from where Figure 1 is borrowed illicitly.

Consider the first of the three plots in Figure 1. It shows Miami's temperature on the day of writing this document (July 3, 2004). The said temperature is plotted as a function of the time of day.

You will notice that the general pattern of the plot is a natural one: The day starts out nearly at its coolest. Then it gets warmer progressively until around 6:00 p.m. when the cooler evening temperatures start to make a showing. This weather-pattern is entirely predictable.

However, if you look more closely at the plot you may notice a myriad of small "wiggles," or "fluctuations," around the said pattern. [The third graph in Figure 1 exhibits an even more pronounced instance of similar this fluctuation phenomenon.] These wiggles seem to be completely random, and are proba-

Figure 1: 2000 seemingly-random numbers



*This work has received partial support from a generous grant from the National Science Foundation.

bly caused by various measurement/instrument errors. Similar random wiggles occur in a vastly-differing number of experimental as well as theoretical works.

This lecture is an attempt to help the student think about randomness. To this end, I will describe two examples, one from dynamical systems, and one from analytic/metric number theory. The point of commonality of these examples is the inevitable way in which randomness creeps into the problem at hand.

2 What does "Random" Mean?

Let us consider the following thought experiment: There is a machine in the corner of a room. If you put in a quarter, then the machine will spew out a number at random. Now imagine that I put in my quarter, and the machine's output was, "0.521." Is this number "random"?

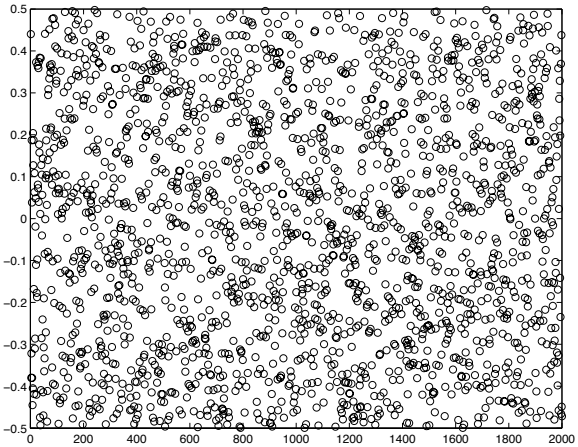
Surely there is nothing random about the number 0.521. By this I mean that any procedure that says, "0.521," will do so again and again, unfailingly and without surprise. [For that matter, 0.098123459082349825 is not random.] What seems to be "random" is the procedure that produced the number 0.521. That procedure is the collection of all of the contortions the machine had to go through before it produced the number "0.521."

And so, a *random variable* is an acronym for the procedure that produces difficult-to-guess numbers. Instead of formally defining random variables, etc., let us plunge ahead and have a look at Figure 2. This figure is based on a certain algorithm that we will study shortly. For now, let us call the mentioned algorithm Newton.

Every time we invoke Newton it returns a number between $-\frac{1}{2}$ and $\frac{1}{2}$. Figure 2 shows the result of 2000 iterations of Newton: On the x-axis we find the iteration number; the y-axis contains the number that Newton returned on that iteration.

At first sight it may seem as if Newton is generating completely random numbers between $-\frac{1}{2}$ and $\frac{1}{2}$. But this is not the case. In fact, Newton is plotting the completely non-random (though very complicated) function that is plotted in Figure 4. Figure 2 is merely evaluating the value of that complicated function F at every integer between 1 and 2000. But F is not just any complicated function. It has the interesting property of being "chaotic." To understand this we need to first know F.

Figure 2: 2000 seemingly-random numbers



3 Newton's Method

Newton's method is a numerical algorithm that finds the root of a nice function f. We are interested in finding a number x_{root} that satisfies $f(x_{\text{root}}) = 0$. In the case that f has several roots we only wish to find one.

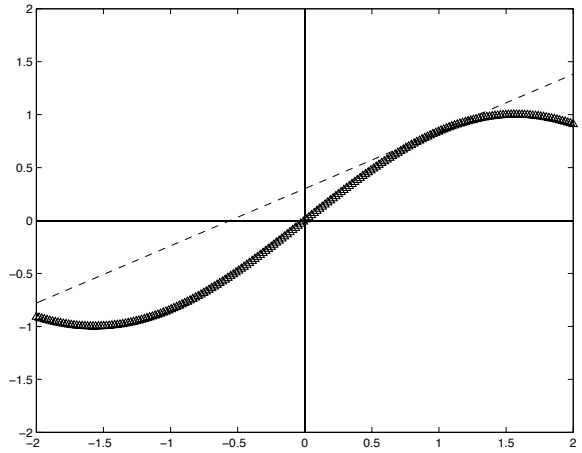
The newton method suggests the following:

1. Start with an initial guess for the root. Call it x_0 (the "seed").

2. We now improve our initial guess x_0 to a better guess x_1. To do this, plot the line that is tangent to the plot of f over x_0. Then x_1 is the root of the said tangent line. A little calculus shows us that if f is a "nice" function, then $x_1 = x_0 - f(x_0)/f'(x_0)$, where $f'(x_0)$ is the slope of the tangent to f at the point $(x_0, f(x_0))$.

3. Start with the guess x_1 and improve it by dropping in the tangent over the point x_1. The root

Figure 3: First Step of Newton's method for $f(x) = \sin(x)$ with $x_0 = 1$



of that tangent line is our next improvement, x_2. That is, $x_2 = x_1 - f(x_1)/f'(x_1)$, where $f'(x_1)$ is the slope of the tangent to f at the point $(x_1, f(x_1))$.

$\vdots$

n. Proceed in like manner, and iteratively define

$$x_n = x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})}, \qquad n = 2, 3 \ldots .$$

If f is a "nice" function, then $x_{\text{root}} = \lim_{n\to\infty} x_n$ exists and $f(x_{\text{root}}) = 0$; i.e., x_{root} is a root of f.

Figue 3 shows the first step in root-finding for $f(x) = \sin(x)$ where $x_0 = 1$. In other words, suppose $x_0 = 1$ is our first guess for a zero of the sine function [plotted with a thick line]. The newton method's first step is to first find the line that is tangent to sine at $x_0 = 1$ [plotted with a dashed line]. Then it sets x_1 to be the zero of the said tangent line [here, $x_1 \approx -0.5774$]. Then x_1 is a second guess for a zero of the sine function. Now proceed by performing the same operations but with x_1 in place of x_0 everywhere. And so on.

3.1 A First Example

Consider $f(x) = x^2$. Then it turns out that $f'(x) = 2x$ for all x, so that the nth stage in the newton algorithm's update is:

$$x_n = x_{n-1} - \frac{x_{n-1}^2}{2x_{n-1}} = \frac{x_{n-1}}{2}.$$

Because the preceding holds for all n we can iterate to compute x_n in terms of the seed. That is,

$$x_n = \frac{x_{n-1}}{2} = \frac{x_{n-2}}{4} = \frac{x_{n-3}}{8} = \cdots = \frac{x_0}{2^n}.$$

So indeed x_n converges to x_{root}, and rapidly.

Question. What does the newton method do to $f(x) = x^2 - 1$? This f has two roots ($x = \pm 1$). Which root does the newton method pick up?

3.2 Another Example

Now we turn to the slightly more complicated example, $f(x) = \sin(x)$. The first step of the Newton method is depicted by Figure 3.

Suppose, as we did earlier, that $x_0 = 1$. It turns out that $f'(x) = \cos(x)$. Therefore, the nth step in the newton method is

$$x_n = x_{n-1} - \frac{\sin(x_{n-1})}{\cos(x_{n-1})} = x_{n-1} - \tan(x_{n-1}).$$

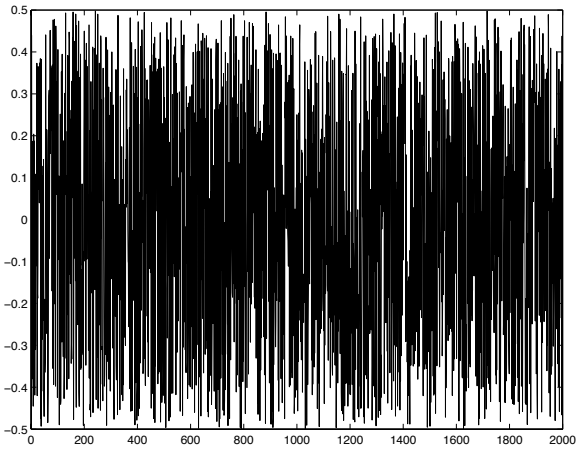
In particular, $x_1 = 1 - \tan(1) \approx -0.5774$; cf. the root of the dotted line in Figure 3. Going further, we successively obtain: $x_2 = x_1 - \tan(x_1) \approx 0.0659$; $x_3 = x_2 - \tan(x_2) \approx -0.0001$; $x_4 = x_3 - \tan(x_3) \approx 0.0000$. So in about four steps we have found that $\sin(0) = 0$. This fact itself is not surprising. The point is that usually Newton's method is very efficient.

3.3 A Chaotic Example

We can also apply the newton method to a function that is nice but has no roots. Such an application is not in the original spirit of Newton's method. Nevertheless, it can produce nice effects.

It is not hard to construct nice functions that have no roots. For instance, consider $f(x) = 1 + x^2$. Before

Figure 4: 2000 runs of Newton's method



we resort to numerical computations let us first explain/predict what happens by relying only on pure though. We start with some x_0; say $x_0 \gg 0$. Then, after a few iterations of the newton-method, we obtain some $x_n \approx 0$. At this point, the slope of f is $f'(x_n) = 2x_n \approx 0$. This means that x_{n+1} is either a very large number, or a very small negative number. We continue on in this way; again after a few runs we come back near zero, get thrown far away from zero, come in, get thrown out, etc.

Of course, we do not expect this process to go anywhere. After all, $f(x) = 1 + x^2$ has no zeros. But what is interesting is that if you change x_0 by a little bit, then a small positive could become a small negative one. So instead of begin kicked out to a very large positive x_{n+1}, all of a sudden the next iteration kicks us out to a very small negative number. This is called *chaos*; it is an emulation of what one might wish to call "randomness."

To demonstrate the thought process of the preceding paragraphs I have run 2000 iterations of the newton method on the computer with $f(x) = 1 + x^2$ and $x_0 = 0.1$. This produces a sequence $x_0, x_1, x_2, \ldots$ which is supposed to have many of the properties of a "random sequence" that takes values between $-\infty$ and ∞. In order to obtain a random-looking sequence with values between $-\frac{1}{2}$ and $\frac{1}{2}$ from this let

$$z_n = \frac{1}{\pi}\arctan(x_n) \qquad n = 1, 2, \ldots .$$

Figure 4 shows a linear interpolation of the sequence $z_0, z_1, \ldots$ when $x_0 = 0.1$ (so that $z_0 = (1/\pi)\arctan(0.1) \approx 0.03173$). Figure 1 depicts the same sequence but does not linearly interpolate. The interesting feature of this particular example is this: The newton method is producing a completely non-random sequence (Fig. 4). But this sequence is so complicated that if we merely plotted the points (Fig. 2) without recording the order in which they came, then the sequence will seem to be random.

4 Normal Numbers

If x is a number between 0 and 1, then we can write in, in decimal form, as

$$x = 0.x_1x_2x_3\ldots ,$$

where the x_j's are integers between 0 and 9.

A number $x = 0.x_1x_2\ldots$ is said to be (simply) *normal* if $\frac{1}{10}$th of the x_j's are zeros, $\frac{1}{10}$th are ones, ..., and $\frac{1}{10}$th are nines. More precisely put, x is normal if for every integer $a = 0\ldots, 9$,

$$\lim_{n\to\infty} \frac{\#\{1 \le j \le n :\ x_j = a\}}{n} = \frac{1}{10}.$$

It is easy to see that such numbers exist. For instance, $x = 0.012345678901234\cdots$ is normal. Other similar equi-distributed patterns of $0, \ldots, 9$ will also work. But what about other, less trivial, examples? For instance,

Are the digits of π normal?

In other words, is $x = (\pi/10)$ normal? You might find it amusing that this 100-year old problem has not been solved [despite repeated attempts].

I know of one non-trivial normal number. Here is the statement:[1]

[1]This was found by a Cambridge (undergraduate) student by the name of David Gowen Champernowne. He wrote this paper in order to obtain a Fellowship at a College at Cambridge. D. G. Champernowne went on to become a well-known economist.

Theorem 1 (Champernown, 1933) *The number* $x = 0.01234567891011121314 15\cdots$ *is normal.*

So by now you might be thinking that normal numbers are so hard to find because there are not many normal numbers. Émile Borel showed that nothing is further from the truth.

Theorem 2 (Borel, 1909) *Let* $\mathcal{N}$ *denote the collection of all normal numbers that are between zero and one. Then the complement of* $\mathcal{N}$ *has length zero.*

It turns out that Theorem 2 is, in fact, a theorem of probability. It can be rephrased as follows:

Theorem 3 (Theorem 2, rephrased) *If we pick a number* X *uniformly at random between zero and one, then* X *is a normal number with probability one.*

To see this, write X in decimal form, $X = 0.X_1X_2X_3\cdots$. Then it turns out that each of the X_j's takes on the values $0,\ldots,9$ with equal probability $1/10$. Moreover, the X_j's are "statistically independent." Roughly speaking, this means that known one or more of the X_j's does not alter the probabilities for the remaining X's. The remainder of Theorem 2 then follows from the law of large numbers of probability theory.[2]

It turns out that the argument that I have sketched here is more useful than Theorem 2 itself. One way to view this argument is this: If $X = 0.X_1X_2X_3\ldots$ is chosen uniformly at random from $[0,1]$, then the X_i's must be statistically independent random variables that take the values $0,\ldots,9$ with probabilities $1/10$ each. Therefore, if we have a random number generator that generates numbers uniformly at random from $[0,1]$, then it must be the case that the digits of the random number must form a truly random sequence with equal probabilities for $0,\ldots,9$. This observation may seem simple, but is at the very heart of nearly all statistical tests of random number generators.

[2] The law of large numbers, in its full generality, is due to A. N. Kolmogorov (1930).