Is Randomness Necessary?*

Ron Graham

What drew me to the study of computation and randomness

As long as I can remember, I have been interested in the search for structure in whatever I encounter. In essence, mathematics can be though of as the science of patterns, so finding them and proving they persist is the bread and butter of mathematicians.

What we have learned

There are many instances where apparent randomness is actually in the eye of the beholder. An example from my own experience is the following. A fellow researcher once came upon a curious sequence in connection with his work on a certain sorting algorithm. It was defined recursively as follows. The first term, call it $x(1)$, was equal to 3. In general, to get the $(n+1)$st term $x(n+1)$, you take the square root of the product 2 times $x(n)$ times $\big(x(n)+1\big)$ and round it down to the next integer value. Thus, the sequence $x(1), x(2), x(3), \ldots$, begins $3, 4, 6, 9, 13, 19, 27, 38, 54, \ldots$. Now, form a new sequence of 0's and 1's by replacing each term in the sequence by the remainder you get when you divide the term by 2. This gives us a new sequence $1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, \ldots$. Suppose now you take every other term of this sequence, starting with the first term. This would result in the sequence (omitting the commas) $S = 10110101000001001111001 10\ldots$. The question was whether anything sensible could be said about S, e.g., would it eventually repeat, are there roughly as many 0's as 1's in it, do all fixed 0/1 blocks occur about equally often, etc. S certainly appeared "random", although it was produced by a fixed deterministic rule. It turns out that we were able to prove that in fact, if you place a decimal point after the first 1, and interpret the result as the binary number $1.01101010000010011110011 0\ldots$, then this is exactly the binary representation of the square root of 2! As a consequence, we know that the sequence is not periodic, for example. Of course, no one can yet prove that the number of 0's is asymptotically equal to the number of 1's as you take longer and longer runs of the bits, and from this

*Appeared in *Randomness Through Computation: Some Answers, More Questions*, H. Zenil, ed., World Scientific Press (2011), 3–5.

point of view, this expansions seems to be behaving like a random sequence. A similar phenomenon may be occuring with Wolfram's "Rule 30". This is a deterministic rule he devised for certain cellular automata which operate on a linear tape which appears to generate sequences with no discernible structure. In fact, it is used in *Mathematica* for generating random numbers, and appears to work quite satisfactory. However, it may be that no one (e.g., no human being) has the intelligence to perceive the structure in what it produces, which actually might well be quite striking.

What we don't yet know

A fundamental technique pioneered in the 1950's by Paul Erdős goes under the name of the probabilistic method. With this technique, one can prove the existence of many remarkable mathematical objects by proving that the probability that they exist is positive. In fact, many of the sharper results on the sizes of such objects are only obtained by using the probabilistic method. However, this method gives absolutely no clue as to how such objects might actually be constructed. It would certainly be wonderful if someone could make progress in this direction.

A recent theme appearing in the mathematical literature is the concept of "quasirandomness". This refers to a set of properties of objects (I'll use graphs as an example), which are all shared by truly random graphs, and which are equivalent, in the sense that any graph family possessing any one of the properties, must of necessity have all the other quasirandom properties as well. It turns out to be relatively easy to give explicit constructions of such quasirandom graphs, which makes it quite useful in many situations in which an explicit construction of a random-like object is desired. One mathematical area where this is especially apparent is in an area of combinatorics called Ramsey theory. The guiding theme in this subject can be described by the phrase "Complete disorder is impossible". Basically, it is the study of results which assert that a certain amount of structure is inevitable no matter how chaotic the underlying space appears. For example, it can be shown that for any choice of a positive number N, there is a least number $W(N)$ so that no matter how the numbers from 1 to $W(N)$ are colored red or blue, in at least one of the colors we must always have an arithmetic progression of equally spaced numbers in a single color. It is of great interest to estimate the size of $W(N)$. The best upper bound known is due to Field's Medalist Tim Gowers and states that $W(N) < 2^{2^{2^{2^{(N+9)}}}}$. The best lower bound known is of the form $W(N) > N2^N$. I currently offer \$1000 for a proof (or disproof) that $W(N) < 2^{(N^2)}$.

The most important open problems

An important trend in computer science is the use of so-called randomization algorithms, i.e., those that have some access to a source of true randomness. It appears

that this increases the range of which problems can be efficiently solved, although it has recently been shown that if there really are computationally intractable problems then randomness cannot be all that helpful. A major open problem is to resolve this uncertain situation. Of course another important problem would be to show how to construct objects now known to exist only with the use of the probabilistic method.

The prospects for progress

I am optimistic that we will be making great progress in tackling many of these questions although it is always hard to predict the timing of such advances. For example, when will the celebrated P versus NP problem be resolved? In our lifetimes? Perhaps. And then again, perhaps not!