Anveshanā • Article • January 2026

Be Wise, Randomize!

by Saraswata Sensarma

"God does not play dice with the universe."

The above quote expresses the discomfort and disdain of Albert Einstein with the stochastic description of the microscopic world in quantum mechanics. He had his reservations about departing completely from a deterministic worldview and deemed quantum mechanics to be an intermediate step towards a *unified field theory*[1], which he spent his final years working on. However, quantum mechanics has undergone extensive experimental scrutiny and immense development since then, and has become fundamental to our understanding of the universe. To the best of our knowledge, the workings of subatomic particles, the very nature of nature itself, is indeed probabilistic. Out of these random dynamics arise the beautifully structured, apparently deterministic phenomena that we observe in our daily lives.

In some sense, this already speaks to the broad applicability of probability theory, which the title of this article alludes to. But what about the macroscopic world, say governed by Newtonian mechanics, which, by its very nature, is deterministic? Can we use probability to address such fundamentally non-probabilistic problems? If so, does it offer any significant advantages? How wide is the scope of applicability of stochastic methods? In this article, we wish to give a semblance of an answer to these questions and hope that these ideas motivate the readers to investigate further on their own. With this premise, we begin our exploration of the applications of probabilistic ideas in various scientific disciplines.

One of the first uses of probability in the physics literature was in statistical mechanics. Consider a gas in a container, with particles large enough so that the quantum mechanical effects have been averaged out. Then, the interaction of these particles follows Newton's laws and thus, at least locally, is reversible. There is no inherent randomness here—if we could somehow figure out the location, mass, and velocity of each particle at a given time, we would know exactly how the system will evolve. Understandably, this is too much information to accumulate or process and thus does not further our understanding of the system. It was in

---

Saraswata Sensarma is a second-year M.Math student at the Indian Statistical Institute, Kolkata. His mathematical interests focus on probability theory and statistical physics. He enjoys exploring other areas of physics, astronomy, and electronics. His corresponding address is sensarma.math@gmail.com.

[1]Einstein wanted to unify gravity and electromagnetism into a single framework, and express both as properties of the spacetime geometry. This would have eliminated the need to consider matter fields and sources separately. He believed this might also explain the origin of quantization from classical geometry.

the second half of the nineteenth century, through the work of Maxwell, Boltzmann, and Gibbs, that a framework to model the macroscopic properties of gases was developed. In essence, they realized that because of the large number of particles in the gas, properties such as volume, temperature, and pressure were barely affected by each individual particle. Instead, it was sufficient to understand how a statistically significant fraction of the particles behaved and how these fractions interacted among themselves. It was this *negligence of the few in favor of the many* that enabled the creation of a statistical theory of gases. These results then formed the basis of a probabilistic foundation of thermodynamics, which was able to explain the long-term irreversibility of thermodynamic systems. Of course, all of this was a big leap of faith, as this molecular picture of gases was yet to be experimentally verified! Indeed, it was the success of this framework that put up a strong case for the existence of molecules.

This is one of the first paradigms where probabilistic ideas came to be used. *If a system depends on a large number of parameters and not too much on any one of them, it may be helpful to randomize these parameters and see what happens*. This applies to many situations in our daily lives- from weather prediction to economics, from social media dynamics to ecology. Of course, the exact model and the randomization procedure will vary depending on the problem at hand. Coming up with an effective model is akin to a work of art—it should be simple enough to be analyzed mathematically while preserving salient features of the system we are after. Paraphrasing Einstein,

> "A model should be as simple as possible, but not simpler."

Let us consider a very different problem. In this day and age, where we routinely send sensitive information via the internet, effective encryption is key. Many encryption methods, like the RSA encryption protocol (developed by Ron Rivest, Adi Shamir, and Leonard Adleman), rely on large prime numbers – the larger the number, the harder the code is to crack. As computers become faster and faster, it becomes crucial to find larger and larger primes to keep our data protected. Say we want to check whether a given natural number n is prime. For starters, if the number is not divisible by any number smaller than itself, it is a prime. After a bit of thought, we realize it is enough to check this up to $\sqrt{n}$. But this still requires a rather long time and becomes infeasible for larger numbers. Can we do better? Consider the following fact from number theory:

> Consider any odd natural number $n = 2^s d + 1$, where d is odd. If n is a prime, then for *every* $1 < a < n$ (henceforth referred to as the base of exponent or simply *base*), either a^d leaves a remainder of 1 or -1, or for some index $1 \leq k \leq s$, $a^{2^k d}$ leaves a remainder of -1. If n is not a prime, then this *fails* for at least $3n/4$ bases $1 < a < n$.

If we can somehow find a base such that this does not work, we can conclude that n is composite. However, doing so would require checking the bases one by one (we may have to

check up to $n/4$ bases). In 1980, Gary L. Miller and Michael O. Rabin presented an innovative solution[2], choosing the index at random from the set $\{2, 3, \ldots, n-1\}$. If n is composite, the probability of choosing an index that happens to work is at most $1/4$. However, repeating this m times and choosing the indices independently at random, the probability that all indices just happen to work is at most $(1/4)^m$. All in all, if we allow for an error probability of ε, this test can be run in merely $C_\varepsilon(\log n)^3$ steps, where the constant C_ε depends on the error threshold. This is quite an improvement from what we had before, which required at least $\sqrt{n}$ many verifications!

This is another paradigm where *the problem is completely deterministic, but employing a random choice and allowing for a small chance of error makes for a fast and efficient algorithm*. Although deterministic algorithms running in polynomial time (around $(\log n)^k$ many steps) are now known[3], the Rabin-Miller test remains the most widely used algorithm to date due to its ease of implementation. The probability of error can be made arbitrarily small, which suffices for most, if not all, applications. This approach also works well for problems where finding a solution is hard, but checking if a guess is indeed a solution is easy. For instance, finding the prime factorization of a large integer is difficult, but verifying a guess requires a few multiplications. This is the very difficulty that guarantees the security of the RSA encryption. If we can find a reasonably fast randomized algorithm that obtains the correct factorization with a large enough probability, repeating it sufficiently many times, we could break the RSA! Fortunately, no such algorithm has been found yet that is implementable on a classical computer.

Let us digress to another, very general class of principles used extensively in combinatorics, aptly called *the probabilistic method*. Say, given a finite set S of objects, we wish to find an object satisfying a given property P. Then one version of the probabilistic method states that: If we can generate a *random* object C taking values in S such that it satisfies P with some positive probability, then there must be at least one object in S satisfying P. While the above statement is almost comically obvious, it can be used to solve problems that are anything but. In this regard, it is somewhat similar to the pigeonhole principle. By cleverly selecting the random object C based on the property P, this often leads to concise proofs and easy bounds. These methods were introduced and extensively used by Paul Erdős and his collaborators to great success, tackling problems in topics ranging from graph theory and combinatorics to number theory, set theory, and discrete geometry. While most applications of this method are simple-minded, they often involve the use of moment methods, concentration inequalities, Lovász's local lemma, or other tools from probability theory. Interested readers are encouraged to check out the book *The Probabilistic Method* by Alon and Spencer, or the earlier book by Erdős and Spencer with the same name.

[2] See the book *Introduction to Algorithms* by Cormen, Leiserson, Rivest, and Stein for more details.

[3] The first such algorithm was developed by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena back in 2002. More details about the story behind this algorithm can be found in an interview of Manindra Agrawal published in the July 2025 edition of the Bhāvanā magazine: https://bhavana.org.in/homegrown-at-iit-kanpur/

Randomness, by its very nature, is unpredictable– making it particularly suitable for cryptography. For example, the RSA algorithm for encryption can be further secured using a probabilistic variant. It is also used in generating digital signatures and zero-knowledge proofs. On the other hand, much like quantum effects averaging out over large scales, many random systems become structured over time, or when sufficiently many random components are involved. This phenomenon is utilized handily in statistics and machine learning, indeed in any discipline where we wish to make predictions based on large amounts of (randomly sampled) data. There are other instances where a deterministic object or value is hard to extract, but we can find a stochastic process converging to it (in an appropriate sense). So long as simulating the stochastic process is reasonably fast, we can carry it on for a long enough time to get better and better approximations to our unknown object! Techniques like Monte Carlo simulation and Monte Carlo integration embody this very idea.

Probability theory is a very flexible branch of mathematics– with applications ranging from the depths of so-called pure mathematics to the most applied of problems. As a final example, consider Brownian motion, named after Robert Brown who first observed pollen grains dancing around in a beaker of water in 1827[4], modeled by Albert Einstein to justify the molecular theory of fluids in 1905, and later formalized mathematically by Norbert Wiener in the 1920s. It somehow becomes the perfect tool to solve the Poisson equation in a bounded domain, an equation fundamental to mathematical analysis, and to numerous branches of the natural sciences. On the other hand, the fact that Brownian motion in two dimensions is recurrent can be used to give a proof of the fundamental theorem of algebra[5]! It is hardly possible to come up with two results so far apart, yet their proofs involve the same foundational tool. Above all the paradigms mentioned before, probability theory has a surprising power of bridging gaps and bringing apparently separate disciplines together in what seems like a divine collaboration—maybe what Erdős would describe as *a proof from The Book* ! I hope these examples indicate the immense power wielded by the simple idea of randomization, which often lies untapped before our very eyes. As we probe deeper and deeper into the microscopic scales of the universe and uncover its non-deterministic nature, maybe we hear it whisper back a suggestion "be wise, *randomize*". Maybe the ability to play dice the right way will open up unexplored avenues and allow us to take a figurative peek into the very mind of God.

[4]In the poem On the nature of things (c. 60 BC), the Roman philosopher-poet Lucretius gives what may be considered an almost perfect explanation for this process but based on a wrong example. See https://en.wikipedia.org/wiki/Brownian_motion for more details.

[5]See the wonderful book *Brownian motion and its Applications to Mathematical Analysis* by Burdzy.