*Corresponding Author:
Email: arup145.roy@gmail.com

Quantum Impossibilities Turn into Useful Tasks: Understanding Power of Quantum Mechanics in Information Science

A Brief Story of Burning Debate to Peaceful Coexistence without Mathematics

Guruprasad Kar[1], Arup Roy[2]*

[1]*Physics and Applied Mathematics, Indian Statistical Institute, Kolkata, West Bengal, India-700108*
[2]*Department of Physics, Hooghly Mohsin College, Hooghly, West Bengal, India-712101*

Abstract: Quantum mechanics, to the broader public, is often introduced through its seemingly paradoxical and counterintuitive principles-most famously the **uncertainty principle**, the **principle of complementarity**, and the **no-cloning theorem**. These ideas have long symbolized the "impossibility features" of the quantum world, setting it apart from the deterministic and predictable framework of classical physics. For decades, such principles fuelled intense debates among both physicists and philosophers, centering on how one should properly *interpret* the nature of quantum reality. However, as the twentieth century drew to a close, a remarkable shift began to unfold. Rather than treating these peculiar features merely as philosophical curiosities or obstacles to understanding, physicists started exploring whether these very strangenesses of quantum mechanics could be harnessed as *resources* for practical use. What emerged from this vision was an entirely new scientific discipline-**quantum information theory** and its technological counterpart, **quantum computation**. This new field reimagines the counterintuitive traits of quantum systems as powerful tools for accomplishing tasks fundamentally impossible within the classical paradigm. Out of this rethinking arose foundational protocols such as **quantum cryptography**, offering unprecedented levels of secure communication; **quantum dense coding**, enabling the transmission of more information using fewer resources; **quantum teleportation**, allowing the transfer of quantum states across distance without physically moving the particles themselves; and **quantum algorithms**, capable of solving certain computational problems at speeds unattainable by any classical machine. In this way, what was once regarded primarily as a domain of abstract puzzles and interpretational controversies has transformed into a vibrant, application-oriented science-laying the groundwork for the future of information, computation, and technology itself.

Keywords: EPR paradox, Bell's theorem, Entanglement, Quantum teleportation

Quantum Revolution

At the dawn of the twentieth century, physics underwent two monumental revolutions, each reshaping humanity's understanding of the universe in profoundly different ways-and both bore the intellectual imprint of **Albert Einstein**. The first was the development of the **theory of relativity**, which sought to reconcile and unify the domains of electromagnetism and mechanics. This gave rise initially to the **Special Theory of Relativity (1905)**, which radically

altered the notions of space and time, revealing them not as absolute, independent entities but as interwoven aspects of a single spacetime fabric. Roughly a decade later, Einstein extended these insights to include gravitation, formulating the **General Theory of Relativity (1915)**, which recast gravity not as a force in the Newtonian sense but as the curvature of spacetime itself. Together, these theories redefined the structure of the physical universe on macroscopic and cosmological scales.

The second revolution stemmed from the **limitations of classical physics** in accounting for experimental observations at the microscopic level. A pressing example was the failure of classical theories to explain the spectral distribution of radiation emitted by a blackbody. This discrepancy, along with a host of other puzzling phenomena revealed in early twentieth-century experiments with subatomic particles and atomic spectra, demanded an entirely new framework. Through sustained efforts to interpret these anomalies, the discipline of **quantum theory** was born.

Yet, while relativity can be viewed as a natural-almost inevitable-extension of scientific reasoning, achieved by incorporating electromagnetism (and later gravitation) into a relativistic framework, **quantum theory represented a dramatic conceptual departure** from the long-held intuitions of classical thought. The principles of relativity, though profound, could still be reconciled with an expanded version of common sense once one accepted the finite speed of light as fundamental. Quantum theory, by contrast, introduced ideas that defied the very logic that had been cultivated over centuries within classical mechanics.

In **classical physics**, the state of a physical system at any given instant is completely specified by the values of its **dynamical variables**. For instance, the state of a point particle is fully determined by its position and momentum-the corresponding point in the **phase space**. From this knowledge, the future trajectory of the particle can be precisely calculated using deterministic dynamical laws, most notably **Newton's laws of motion**. This framework embodies the classical belief in causality, predictability, and determinism.

Quantum mechanics, however, would soon reveal that this classical worldview was only an approximation-a surface description of a much stranger and richer underlying reality [1].

What is Quantum Theory?

In **quantum theory**, the description of nature takes on a level of abstraction and subtlety that is fundamentally different from the intuitive picture offered by classical physics. The experimental discoveries of the early twentieth century-such as the **wave-like interference pattern of particles in the double-slit experiment**, the **discrete spectral lines emitted by atoms**, and a variety of other phenomena-could not be reconciled within the framework of Newtonian mechanics or Maxwell's electrodynamics. These results compelled physicists to construct an entirely new mathematical formalism, one capable of capturing the strange dualities and statistical behaviours that experiments consistently revealed.

In this formalism, the **state of a quantum system** is no longer defined by a set of definite values of dynamical variables such as position or momentum. Instead, the state is represented by a **vector in an abstract Hilbert space**. Rather than yielding sharp values of physical quantities, this state provides the **probability distributions** for the outcomes of measurements of all possible observables. Thus, quantum mechanics departs from the deterministic worldview of classical physics and replaces it with a framework in which probability and measurement play central roles.

Among the many striking features of this new theory, a few stand out for their philosophical and practical significance. One such cornerstone is the **Heisenberg Uncertainty Principle**. It asserts that it is impossible to prepare a quantum state in which both the uncertainty in position and the uncertainty in momentum can be made arbitrarily small simultaneously. Mathematically, the product of these uncertainties is bounded below by a fundamental constant (Planck's constant, divided by 4π), signifying a built-in limitation of nature rather than a shortcoming of experimental precision.

Closely related to this is **Bohr's Principle of Complementarity**, which emphasizes the mutually exclusive nature of certain dynamical quantities. For instance, position and momentum cannot be measured jointly with arbitrary accuracy, and more broadly, quantum systems exhibit both **particle-like properties** (localization) and **wave-like properties** (delocalized interference). However, these dual aspects cannot be observed simultaneously in a single experimental arrangement. The choice of measurement setup determines which aspect-particle or wave-is revealed, underscoring the context-dependent nature of quantum phenomena.

Another profoundly important feature of quantum mechanics concerns the **role of measurement itself**. Unlike in

classical physics, where measurement is regarded as a passive act that merely reveals preexisting properties, in quantum mechanics the act of measurement generally **alters the system irreversibly**. Upon measurement of a particular observable, the system is said to undergo a transition into a new state-known as the **post-measurement state**-in which the measured observable attains a definite value. This sudden and non-deterministic change of state is captured by what is known as the **collapse postulate**. It represents one of the most conceptually puzzling aspects of quantum theory, raising deep questions about the role of the observer, the boundary between the microscopic and macroscopic worlds, and the very meaning of reality [1].

Is it possible to have deeper level of description than quantum mechanics?

One of the most **puzzling and controversial features** of quantum theory lies in its departure from the classical notion of physical reality. In quantum mechanics, the state of a system does not assign definite values to measurable quantities such as position or momentum. Instead, it encodes only the **probabilities** with which different outcomes may be revealed upon measurement. This probabilistic character of the theory disturbed many leading physicists of the time, most notably **Albert Einstein**, who remained deeply sceptical throughout his life. Einstein could not accept quantum mechanics as a **complete theory of individual systems**; to him, it seemed more like a statistical framework describing ensembles rather than the fundamental truth about nature itself.

This skepticism culminated in 1935, when Einstein, together with **Boris Podolsky and Nathan Rosen**, published their famous paper-now known as the **EPR paradox**. In this work, they argued that quantum mechanics must be incomplete. Their reasoning was built upon two key assumptions: a **reality condition** and a **locality condition**. The reality condition stated that if one can predict the value of a physical quantity with certainty-without disturbing the system-then that quantity must correspond to an element of reality. Their version of this condition was, in fact, more general than the framework allowed by standard quantum mechanics. The locality condition, on the other hand, asserted that events occurring at one place cannot instantaneously influence events at another spatially separated location.

From these premises, Einstein and his collaborators concluded that quantum mechanics fails to provide a complete description of reality. The implication was that perhaps **every individual system does indeed reside in a definite state**, with sharp values assigned to all measurable quantities, but the theory we possess—quantum mechanics-only reflects an **incomplete knowledge** of these systems. According to this view, the quantum state is merely a **statistical mixture** of more fundamental states, which include not only the known variables but also additional, as-yet-undiscovered parameters. These hypothetical parameters came to be known as **hidden variables**, and it was hoped that a deeper theory incorporating them would restore determinism and completeness to physics.

It is crucial, however, to recognize that neither the **uncertainty principle** nor the **complementarity principle** by themselves rule out such a deeper level of description. The uncertainty principle simply states that it is impossible to prepare an **ensemble of systems**, all in the same quantum state, in which both the position and momentum are simultaneously defined with arbitrary precision. Yet this does not logically exclude the possibility that an **individual particle** may, in reality, possess definite values of both position and momentum-values that are merely inaccessible to us within the current framework. Similarly, the principle of complementarity asserts only that certain quantities, such as position and momentum, cannot be **jointly measured** within a single experimental arrangement. It does not establish that particles cannot have well-defined values of these quantities independent of measurement.

Thus, while quantum mechanics introduced radical new principles that challenged classical intuition, it left open the philosophical and scientific question of whether it was a **complete description of nature** or merely an effective statistical theory awaiting a deeper, hidden structure [1].

Local realistic theory can not reproduce quantum mechanics

In 1964, the physicist **John Bell** made a discovery that profoundly altered the debate surrounding the foundations of quantum mechanics. He demonstrated that if one assumes **locality**-the principle that no physical influence can travel faster than light, so that a measurement performed on one system cannot instantaneously affect the outcome of a distant system-then, combined with the **reality assumption** (the idea that every individual system possesses definite values for

all measurable quantities, regardless of whether we observe them), this framework necessarily leads to certain **observable consequences**. These consequences, however, are in direct conflict with the predictions of quantum mechanics.

This insight was revolutionary. For the first time, Bell showed that the philosophical dispute about whether quantum mechanics is "complete" could be settled not merely by thought experiments but through **real laboratory tests**. His result transformed the discussion from a matter of interpretation into one of empirical science: if experiments confirm quantum predictions, then no theory based on locality and preassigned definite values (so-called **local hidden-variable theories**) can be true.

To understand the depth of Bell's result, let us describe a simple but illustrative **experimental arrangement** and analyze the outcomes both from the quantum-mechanical perspective and from the standpoint of the locality and reality assumptions.

Suppose we have a **source**, denoted by SSS, that emits **three particles simultaneously** during each trial (see Fig. 1). These three particles are directed towards three separate measurement devices, labelled as M, N, and P. These devices are assumed to have no connections with one another; in principle, they could even be separated by **vast cosmic distances**, light-years apart, ensuring that no signal could pass between them in the short interval of measurement.

Each measuring device has a **dial** with two possible settings, labelled **A** and **B**. When a particle arrives at one of these machines, the device performs a measurement according to the dial setting and then produces an outcome, signalled by a light flash. There are two indicator bulbs on each machine: one red (R) and the other green (G). For each incoming particle, and for whichever dial setting is chosen, **exactly one bulb flashes**-either red or green.
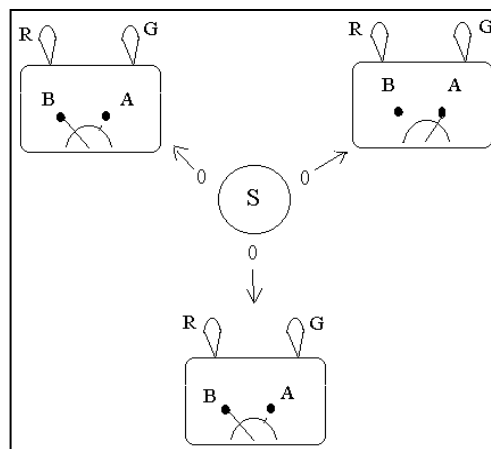
Each emission of three particles from the source S constitutes an **experimental run**. During a run, the dial settings on the three machines are chosen randomly and independently (either A or B for each machine). The complete record of the experiment thus consists of:

1. The **dial settings** of machines M, N and P during that run, and
2. The **outcomes** (red or green) that each machine registers.

By accumulating data over many such runs, one can compare the **statistical patterns** predicted by quantum mechanics with those permitted under the joint assumptions of locality and realism. Bell's remarkable theorem asserts that the two sets of predictions are fundamentally incompatible: there exist correlations between the outcomes of distant machines which quantum mechanics predicts but which no local realistic theory can reproduce.

Suppose that the experiment has been performed many times and data have been collected. Let us assume that the data analysis reveals the following:

(1) In those runs where two of the machines were in setting B and one in A, the results (flashing either red or green) are without exception as follows;
    Either two flash green(G) and one red (R) or all flash red (R).

(2) In those runs where all the machines were in the setting A, the results are, again without exception, are as follows;
    Either two flash red (R) and one green or all of them flash green (G).

Figure 1. Either two flash red (R) and one green or all of them flash green (G)

Now immediately it happens to one that in the source the particles can be instructed and correlated in such a way as to reproduce the above results. One should remember that machine settings are completely random and so can not have any correlation with the instructions given to the particles in the source. And also there is no nonlocal effect in the sense that after being fired any particle flashing in its machine can in no way influence other to act in a way other than as has been instructed initially. Below we are presenting a set of eight instruction [(a) –(h)] which reproduces the result in (1) (see table-1).

Table 1. A set of eight instruction [(a) –(h)]

		1	2	3			1	2	3
a)	A	R	R	R	e)	A	G	R	G
	B	G	G	G		B	R	G	R
b)	A	G	R	G	f)	A	R	G	G
	B	G	R	G		B	G	R	R
c)	A	G	G	R	g)	A	G	G	R
	B	G	G	R		B	R	R	G
d)	A	R	G	G	h)	A	R	R	R
	B	R	G	G		B	R	R	R

To illustrate Bell's insight more concretely, let us first imagine a **classical-type instruction set** carried by the particles. For example, suppose particle 1 is emitted with the rule: *"If the machine setting is AAA, flash Red (R); if the setting is BBB, flash Green (G)."* Similarly, particles 2 and 3 are assigned their own instructions. In this picture, each particle leaves the source already carrying a definite prescription for how it should behave under either setting of its respective machine.

If we try to explain a particular pattern of correlations-say, result (1)-we can identify a set of such deterministic instruction tables. One can enumerate all possibilities, and in this case it turns out that there are exactly eight distinct instruction states which exhaustively reproduce the outcomes of (1). Thus, one might reasonably assume that on each run, the source emits the three particles in one of these eight possible states (or, more generally, in some statistical mixture of them).

However, when we attempt to account for result (2), a difficulty arises. None of the eight instruction states that reproduce (1) can yield (2). Conversely, if we design a new instruction set to reproduce (2), it becomes impossible to reproduce (1). From a classical point of view, this incompatibility seems unavoidable: **no locally pre-programmed set of instructions** can simultaneously explain both types of correlations, provided that there is no conspiracy (i.e., no correlation between the random choice of machine settings and the state preparation) and no faster-than-light influence among the machines. In the **classical world**, this reasoning holds: incompatible outcomes simply cannot be produced under those constraints.

Yet, the **quantum world defies this logic**. If we consider three spin-1/2 particles (such as electrons) emitted from a common source, and replace the machine dials AAA and BBB with spin measurements along two **orthogonal polarization directions**, the outcomes can exhibit precisely the sort of apparently contradictory correlations described above. Each measurement yields one of two possible results, "spin-up" or "spin-down," analogous to the red and green flashes. What enables such behaviour is not hidden instructions but rather the presence of a uniquely quantum phenomenon: **quantum correlations**, often referred to as **entanglement**.

These quantum correlations are fundamentally different from any classical correlations, no matter how subtle. They cannot be explained as arising from pre-existing hidden instructions carried by the particles, nor as the result of statistical mixtures of definite states. Instead, they arise from the holistic nature of the quantum state shared by the particles, a state in which the outcomes of measurements on different subsystems are deeply interdependent, even when

the subsystems are separated by large distances.

This is precisely the power of **Bell's theorem**. Bell showed that if one interprets quantum mechanics as a merely statistical theory—analogous to how classical statistical mechanics sits atop deterministic classical dynamics—then any such deeper deterministic theory would be forced to abandon **locality**. In other words, if hidden variables exist, they must allow influences that stretch across space instantaneously, violating the classical idea of local causality.

At the same time, it is crucial to distinguish between two different senses of "non-locality." Quantum mechanics does not permit **instantaneous signalling** or communication faster than light; the statistical outcomes observed by one observer cannot be used to transmit usable information to another at spacelike separation. Instead, quantum theory is "non-local" only in the more subtle sense that **no local realistic theory-no matter how cleverly designed—can reproduce its predictions**. Thus, quantum mechanics forces us to rethink the very structure of reality: nature is neither purely local nor classically realistic, but instead governed by the uniquely non-classical logic of entanglement [1,2].

No Cloning theorem

Amidst these conceptual breakthroughs in the foundations of quantum mechanics, yet another striking result emerged in 1982, due to **Wootters and Zurek**, which has since become famous as the **No-Cloning Theorem**. Despite its apparent simplicity, this result carries profound consequences for our understanding of quantum systems and, more importantly, for the development of modern **quantum information theory**.

The theorem states that it is impossible to construct a **universal machine** that can make a perfect copy of an **arbitrary unknown quantum state**. In other words, given a particle prepared in some unknown state $|\psi\rangle$, there exists no physical process that can reliably produce two identical particles, each in the state $|\psi\rangle$. This prohibition against cloning is not a matter of technological limitation but a **fundamental law of nature**, arising directly from the linear structure of quantum mechanics.

The implications of this result are far-reaching. First, it tells us that an **unknown quantum state cannot be fully determined**. To identify a state completely, one would need to make many identical copies of it and perform different measurements on those copies. Since perfect cloning is forbidden, there exist quantum states that are distinct yet impossible to distinguish with certainty in a single measurement. This stands in stark contrast to the **classical world**, where a state-say, the position and velocity of a particle-can in principle be measured exactly and then copied without restriction.

At first glance, the No-Cloning Theorem may appear to be a technical curiosity, but its significance is enormous. It underpins the very security of **quantum cryptography**, where the impossibility of copying an unknown state ensures that an eavesdropper cannot secretly intercept and duplicate quantum signals without leaving a trace. It also shapes the architecture of **quantum communication** and **quantum computing**, by placing fundamental constraints on how information can be processed and transmitted in the quantum domain.

Thus, what began as a seemingly simple theorem has evolved into one of the **cornerstones of quantum information theory**, influencing both our theoretical understanding of quantum states and the design of revolutionary technologies that exploit their uniquely non-classical properties [3].

Laws of Quantum Mechanics Enter into Information Theory

Having outlined some of the foundational principles of quantum mechanics, we now turn our attention to exploring their applications within the emerging field of **quantum information theory**. Yet, before delving into these applications, one must carefully recognize the sense in which the laws of quantum physics enter into the domain of information processing.

It is important to recall that, long before the formal emergence of quantum information science, the insights of quantum mechanics had already been instrumental in shaping and advancing technology. For instance, the miniaturization and acceleration of silicon-based or other semiconductor devices owe their success to a sophisticated understanding of the quantum behaviour of electrons in solid-state systems. Similarly, superconductivity—an intrinsically quantum

phenomenon—has been exploited to enhance technological efficiency, providing benefits such as faster digital switching speeds and reduced power consumption. However, these achievements, while remarkable, do not represent a **fundamental conceptual departure** from classical technology. The logical operations that underlie the manipulation of physical bits in such devices continue to conform to the established framework of classical information theory. In other words, these advancements reflect quantum physics improving our existing tools, but not fundamentally altering the logical structure of information processing.

A truly **revolutionary transformation** arises when the peculiar and counterintuitive laws of quantum mechanics-such as superposition, entanglement, and the no-cloning theorem-are allowed to reshape the very foundations of information theory itself. This shift entails moving beyond merely optimizing classical devices and instead envisioning machines that process, store, and manipulate information **inherently according to quantum principles**. In such devices, the very building blocks of information-the so-called *quantum bits* or *qubits*-obey rules fundamentally distinct from those of their classical counterparts. Consequently, the operations performed within these systems, and the logic they embody, would inaugurate a wholly new form of information technology: one that is not simply an improved extension of classical methods, but a **radical departure into a new paradigm** of computation and communication [3].

Quantum Cryptography

The most straightforward yet remarkably powerful application of quantum principles in the field of information processing lies in **cryptography**. At its core, cryptography is concerned with the **secure exchange of information** between two parties in such a way that any external attempt to intercept, eavesdrop, or break the code becomes futile. In a typical cryptographic scheme, the foundation of security is built upon the notion of a **shared secret key**. The sender encodes the message using this key, and the receiver—who possesses the same key—decodes it to reconstruct the original message. This model of communication is not merely theoretical; it has long been employed in practical systems and remains a cornerstone of digital security today.

Traditionally, the problem of establishing such a key was resolved in a very physical and straightforward manner: the two parties would meet in person, agree upon a shared key, and later use it for secure communication when separated by distance. While effective in small-scale or controlled environments, this solution quickly becomes impractical in situations where the communicating parties are located far apart or when frequent secure communication is required. This naturally raises a crucial question: **is it possible to generate or exchange a secure cryptographic key when the two parties cannot meet physically?**

In the realm of **classical communication**, the answer is troubling. Any classical communication channel can, in principle, be monitored **passively**, meaning that an eavesdropper could intercept information without leaving behind any evidence of intrusion. To illustrate, consider the scenario in which a cryptographic key is delivered by a trusted courier. Even before the courier reaches the recipient, the key might have been secretly copied using advanced methods such as high-resolution X-ray imaging or other non-invasive techniques—without the courier or the communicating parties being aware of the breach. This vulnerability arises because, in classical physics, **all information is encoded in measurable physical properties**—such as the ink on paper, the magnetic orientation of bits, or the voltage of signals. Classical theory permits, at least in principle, the precise measurement of these properties without altering them, leaving the door perpetually open to undetectable eavesdropping.

Here lies the fundamental weakness of classical cryptography. But it is precisely at this point that **quantum mechanics offers an elegant and revolutionary solution**. By employing the laws of quantum systems in the generation and exchange of secret keys, one can eliminate the possibility of undetected interception. In quantum cryptography, the message-or more specifically, the key informationis encoded in the **quantum states** of particles such as photons. A profound principle of quantum mechanics asserts that an **unknown quantum state cannot be perfectly cloned or measured without disturbance**. Thus, if an eavesdropper attempts to intercept and measure the quantum system carrying the information, the act of measurement itself will inevitably and irreversibly disturb the system.

This disturbance is not merely theoretical-it provides a practical mechanism for detection. When the sender and receiver later compare a subset of their measurement results against the original preparation of the states, any discrepancies will immediately reveal the presence of an intruder. In this way, quantum cryptography makes **passive monitoring fundamentally impossible**: the very laws of nature guarantee that eavesdropping cannot remain hidden.

Therefore, quantum systems transform the landscape of secure communication. Where classical cryptography leaves vulnerabilities exposed, quantum cryptography offers not only secrecy but also **inviolable assurance**, grounded in the immutable principles of quantum mechanics [3].

Quantum Teleportation

The most remarkable breakthrough that firmly established **quantum entanglement** as a genuine resource for quantum information science is the phenomenon known as **quantum teleportation**. To the uninitiated, the very term evokes the imagery of science fiction, where teleportation is often portrayed as a miraculous process. In fictional narratives, teleportation typically proceeds in the following manner: a sophisticated device scans an object or a person, extracting every possible detail required to describe it completely. This exhaustive dataset is then transmitted to a distant receiver, where an identical replica of the original is reconstructed, as though the original had been instantaneously transported across space.

At first glance, however, such a scheme seems entirely incompatible with the principles of **quantum mechanics**. The very foundation of the theory dictates that an **unknown quantum state cannot be fully determined through measurement**, since the act of measurement itself irreversibly alters-and, in fact, destroys-the delicate quantum superposition that defines the state. According to this line of reasoning, teleportation should be fundamentally impossible. Yet, in 1993, to the astonishment of the scientific community, a team of physicists overturned this conventional wisdom. They demonstrated that teleportation is indeed possible-not by evading the rules of quantum mechanics, but rather by exploiting them. The key lies in **quantum entanglement**, a uniquely non-classical correlation between two or more particles that allows them to share a single, inseparable quantum state.

To illustrate this idea, consider two distant parties, traditionally named **Alice** and **Bob**, who share an entangled pair of particles. Suppose Alice is given a third particle prepared in an **unknown quantum state**, and her task is to reproduce that state at Bob's location-without physically sending the particle itself. At first this sounds paradoxical, but remarkably, a universal protocol makes it possible. Alice performs a specific type of joint measurement on her two particles: the unknown particle and her half of the entangled pair. The outcome of this measurement, though random, contains information that Alice can communicate to Bob using ordinary classical means. Upon receiving this information, Bob applies a corresponding transformation to his own particle. The result is extraordinary: Bob's particle now assumes **precisely the quantum state that Alice's unknown particle originally possessed**, while Alice's side is left with no trace of it-thus upholding the **no-cloning theorem**, which forbids the creation of identical copies of an unknown quantum state.

The theoretical prediction of quantum teleportation soon transitioned from the abstract to the tangible. In 1997, the first **experimental demonstration** of quantum teleportation was achieved using photons, with their **polarization states** serving as carriers of the quantum information. This achievement was not merely a technical triumph; it signaled the dawn of a new era in quantum information processing. At the same time, it reaffirmed the profound validity of the standard interpretation of quantum mechanics-rooted in the principles of **superposition** and **wavefunction collapse**-which, once again, proved consistent with experimental reality.

In this way, quantum teleportation transformed what once seemed like the domain of science fiction into a concrete scientific possibility, demonstrating both the power and the subtlety of the quantum world [4].

Quantum Computation

Perhaps the most striking and revolutionary application of **quantum correlations** lies in the domain of the **quantum computer**. A fully realized quantum computer has the potential to bring about an **exponential acceleration in computational efficiency** for certain classes of problems that are otherwise intractable with classical machines. A paradigmatic example is the problem of **prime factorization of very large integers**-a task that underpins the security of modern cryptographic systems. Whereas classical algorithms require an enormous amount of time to factor such numbers, a quantum computer could, in principle, accomplish this exponentially faster.

The foundation of this remarkable capability rests on two quintessential principles of quantum theory: the **superposition principle** and **quantum entanglement**. Together, they enable what is known as **quantum parallelism**, a feature that arises naturally in the mathematical framework of the **tensor product structure of Hilbert spaces** describing multipartite quantum systems. In essence, while a classical computer bit exists deterministically in one of two states (0 or 1), a **quantum bit (qubit)**-such as the spin state of an electron-can exist in a linear superposition of both basis states. Extending this idea, a system of n qubits does not merely encode one of 2^n possible configurations, but instead represents a **superposition of all 2^n states simultaneously**.

It is precisely this exponential growth of accessible states with linear increases in system size that gives quantum computation its extraordinary power. To appreciate the contrast, consider classical parallelism: in conventional computing, the execution time for a complex task can be reduced by deploying multiple processors to handle parts of the problem concurrently. However, to achieve an exponential reduction in time using classical parallelism would require an **exponential increase in the number of physical processors**, which in turn demands an exponential amount of physical resources and space. By contrast, in a quantum system, the **degree of parallelism increases exponentially with the number of qubits**, yet the required physical resources scale only linearly. This profound efficiency is what elevates quantum computation far beyond classical limits.

The situation can be illustrated with the example of **function evaluation**. In a quantum computer, with n qubits one can, in principle, evaluate a function over all 2^n input points **in a single operation**. A classical computer, by comparison, would require 2^n distinct steps to achieve the same result. However, this remarkable advantage comes with a subtle but fundamental limitation: the results of the computation exist only in a **quantum superposition**. Any direct attempt to measure the state collapses the superposition, yielding the function value at only **one randomly chosen point**, thereby erasing the advantage and reducing the process to its classical analogue.

The true power of quantum algorithms emerges not from reading out all these exponentially many results directly, but from exploiting the **global properties encoded in the superposed state** before measurement. Ingenious algorithmic strategies are designed to extract structural or global information about the function-properties such as **symmetry, periodicity, or hidden correlations**-without ever needing to access each value individually. For example, **Shor's algorithm** for integer factorization harnesses quantum interference to determine the **period of a certain function** related to modular arithmetic. By cleverly exploiting this periodicity, the algorithm transforms the seemingly insurmountable task of factoring large numbers-a problem that would take astronomical time on classical machines-into one that becomes efficiently solvable on a quantum computer.

Thus, quantum computation does not merely represent a faster version of classical computation. Rather, it embodies an entirely new paradigm of information processing-one that redefines the very limits of what can be computed in practice [3].

The last word

Since antiquity, philosophers and scientists have been engaged in profound debates concerning a central question: *Do the finest theories emerge from pure reasoning and abstract logic, with nature merely conforming to these pre-established structures? Or, conversely, do reason and logic themselves evolve out of humanity's empirical encounters with the natural world, shaped by countless experiments, practices, and interventions?*

The historical development of **quantum mechanics** offers a decisive perspective on this debate. It demonstrated beyond doubt that logic and reason are not immutable, timeless frameworks handed down once and for all. Rather, they are dynamic, continually reshaped and refined in response to new experiences and experimental discoveries. The conceptual foundations of **classical physics**, which had long governed our rational understanding of the universe, proved insufficient when confronted with the surprising and often paradoxical phenomena revealed in the atomic and subatomic domains.

In this new scientific landscape, the **logic of quantum theory**, with its counterintuitive principles-such as superposition, entanglement, and uncertainty-emerged as a necessity rather than a choice. Initially unsettling to established reason, these principles have since been rigorously validated by a wealth of sophisticated experiments and precise measurements. What is more remarkable, however, is that this novel form of logic does not merely explain nature-it opens unprecedented pathways to **manipulate and harness natural processes** in ways previously unimaginable. By

embracing the quantum mode of reasoning, human society gains the capacity to **expand its technological and productive capabilities**, transforming both the theoretical foundations of science and its practical impact on civilization.

References

1. Mermin ND. Hidden variables and the two theorems of John Bell. Review of Modern Physics 1993, 65: 803.
2. Bell JS. Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press, Cambridge, 2014.
3. Nielsen MA, Chuang I. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 2000.
4. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters 1885, 70:1895.