Applications of quantum computing

Many quantum algorithms have been evolved for quantum computers that deliver speedup which is a result of some fundamental mathematical methods like Fourier transform, Hamiltonian simulation, etc. Most algorithms require a large number of qubits of the best quality and some error correction to provide use-
ful functionalities. These algorithms are formed in blocks rather than as a whole combined application since it is not practical. Therefore, it is a great challenge to create quantum applications that are really practically useful along with providing speedup with no error. The potential utility or say useful application of a quantum computer is an area of ongoing research. It is predicted that those applications require fewer qubits and can be carried out with a lesser amount of codes. It is pos-sible to build algorithms that can run faster on quantum computers because of the distinct features of the qubit. Below are some of the primary applications that we will see soon in the upcoming era:

- **Cryptography**

Many important elements of IT security and online security such as e-commerce and electronic secrecy depend on encryption and mathematical algorithms which are difficult to break such as factoring very huge numbers into primes (RSA tech-nique). It is done by traversing through every possible factor using conventional computers which takes a significant amount of time. Also, some modern algorithms other than RSA like AES, ECDSA, etc. cannot be cracked using even high com-puting power. It makes it costly and cracking them even less practical. Quantum computers can do all these kinds of stuff in exponentially less amount of time.
New quantum algorithms (e.g. Shor's algorithm) are able to do it and more unique algorithms will develop. But before that, new encryption techniques are being made to resist the quantum ones. Since the already running techniques and digital applications security are at greater risks.

- **Optimization Problems**

Optimizing a problem implies finding the best solution to that problem out of all the possible solutions. It can be done by minimizing the error and even minimizing the steps available. Quantum computers are best in solving optimization problems. There are a lot of quantum algorithms out of which quantum optimization algorithms might improve the already existing optimization problems which are solved using conventional computers currently. Some of them are quantum semi-definite programming, quantum data fitting, and quantum combinatorial optimization.
Some of the examples include simulating the molecular model like protein behavior for medical research which can lead to the new discovery of drugs for serious dis-eases like cancer, lung disease, etc. Another example is the Simulation of the cellular structure of batteries for improving battery power and life in electric vehicles.

-

It could also solve travel-related problems in real traffic just like traveling salesman problems to find the shortest path between many cities, going to each city once and returning back, modeling the entire finance market, and many more. Traveling optimization is the major work under Volkswagen recently .

- **Artificial Intelligence**

Artificial Intelligence counts on processing large and complex datasets. It is responsible for learning, inferring, and understanding. It learns until it stops

mistaking and making errors in its task. It takes a significant amount of time in learning too. But quantum computing can make it easy and more accurate. Since conventional computers are only training the learning model from a specific size of the dataset to restrict the computation time. Quantum computers can train these models over a huge dataset without sticking into the exponential time. The more data it uses to train, the more accurate it will be. Generative models generate output such as image, audio, etc. that can be fed to quantum computers to improve its quality and accuracy. Natural Language processing is another example that can

understand complete sentences. Quantum computers can make it understand all the phrases and speech in real-time with improved quality, which is computationally costly with today's computer.

- **Quantum Simulation**

It is an important utility in the field of quantum chemistry and material science [31]. This problem needs solving ground state energies of electrons and their wave functions, with or without the presence of some external electric or magnetic field. From the structure of atoms and electrons in chemistry to the rate at which chemi-cal reactions are taking place, everything can be simulated very well. The classical computer when applied to this problem often fails to reach the level of precision needed to predict the rate of the chemical reaction. It could also have commercial applications in areas such as medical and health-care fields, chemical catalysts, storage of energy, pharmaceutical advancement and device displays.

Quantum Measurement

Definition

Quantum measurement is the physical process by which classical information (a definite value, such as 0 or 1) is extracted from a quantum system that exists in a superposition of states. It is the interaction between a quantum system and a measuring device (or the environment) that forces the system's wave function to **collapse** into one definite, observable outcome, with a probability predicted by quantum theory rather than known in advance.

Qubits, Superposition and the Wave Function

- A **qubit** (quantum bit) is the basic unit of quantum information. Unlike a classical bit, which is always definitely 0 or 1, a qubit can exist in **quantum superposition**, simultaneously holding probability amplitudes for both 0 and 1.
- Before measurement, the qubit is described mathematically by a wave function (state vector), which represents the probabilities of each of its potential states — it does not itself correspond to one classical value.

The general single-qubit state is written as:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{(i\varphi)} \sin(\theta/2)|1\rangle$$

Example — for $\theta = \pi/2$, $\varphi = 0$ (equal superposition):

$$|\psi\rangle = (1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$$

Here, measuring the qubit gives outcome 0 with probability 1/2 and outcome 1 with probability 1/2.

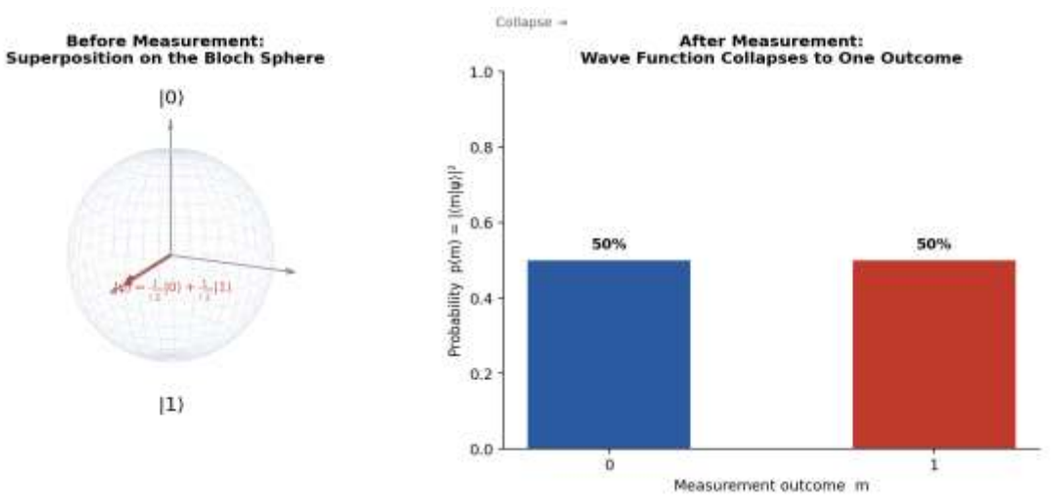


Fig 1: Superposition on the Bloch sphere (left) collapses to one definite classical outcome upon measurement (right).

3. Diagram — The Measurement Process

Quantum measurement can be represented as a pipeline: a qubit state passes through a measurement device, which outputs a classical result.

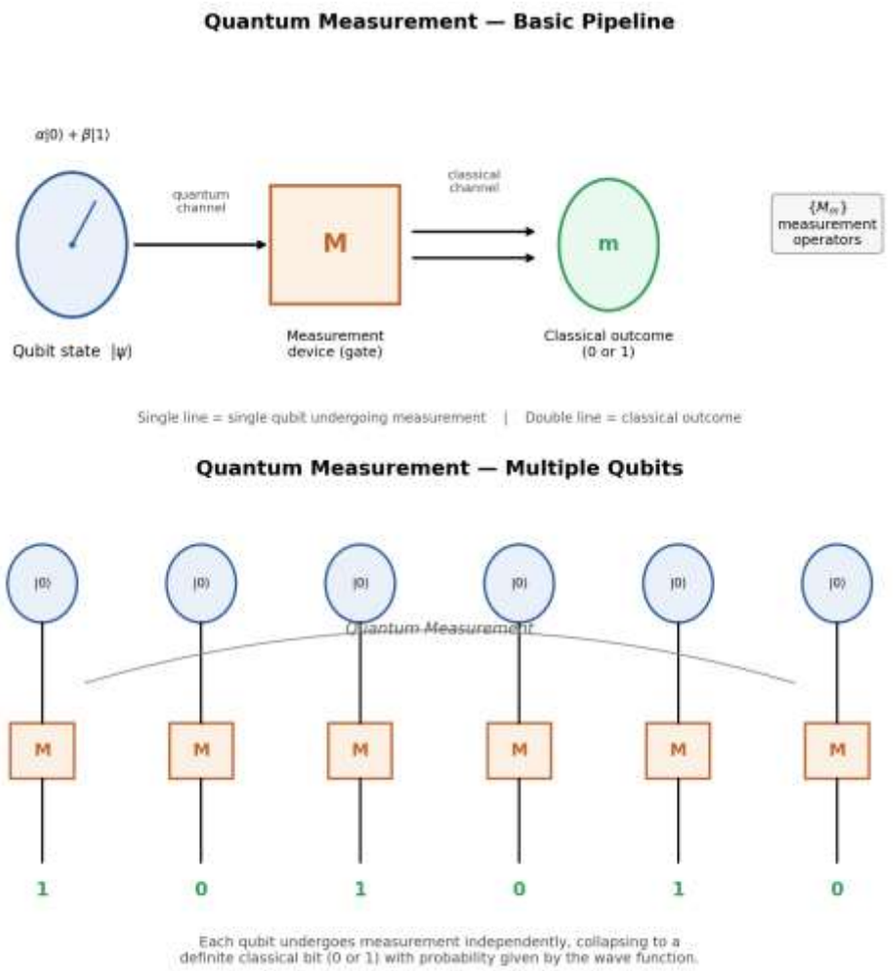


Fig 2: A single line denotes a qubit (quantum channel); a double line denotes the classical outcome (classical channel) after measurement. {M□} is the set of measurement operators.

For the simplest case — projective measurement in the computational basis — M□ = |m⟩⟨m|, so the Born rule reduces to p(m) = |⟨m|ψ⟩|². Measurement thus decisively determines the qubit's state as either zero or one, collapsing the wave function irreversibly.

Why Quantum Measurement Is Probabilistic

- A single measurement yields only one random sample of the underlying probability distribution, not the full quantum state.
- Because outcomes are probabilistic, systems are often repeatedly prepared, reset, and measured to obtain accurate statistics (many 'shots').

Analogy (Schrödinger's Cat): *Until the box is opened, the cat is in superposition — simultaneously (i) dead and (ii) alive. Opening the box is the measurement — it forces one definite, classical outcome.*

Applications / Significance

- Extracting the final classical answer from quantum algorithms (e.g., Shor's, Grover's algorithm).
- Quantum error correction: partial (syndrome) measurement of ancilla qubits reveals error information without collapsing the encoded data qubit's superposition — critical for fault-tolerant quantum computing.
- Quantum cryptography (QKD), where measurement statistics reveal the presence of eavesdropping.
- Quantum sensing and metrology, where measurement precision determines device performance.

Quantum measurement is the fundamental process that bridges the quantum and classical worlds — collapsing a qubit's probabilistic wave function into one definite, observable bit. It underlies how we read out results from quantum computers, why quantum algorithms are inherently statistical, and why techniques like repeated sampling and partial measurement (for error correction) are essential to practical quantum computing.