QUANTUM COMPUTING: BASIC THEORY AND ELEMENTS

Sumit Kumari

(Sunrise University Alwar)

(Sumitjania02@gmail.com)

ABSTRACT

Quantum computing is a new type of science that uses special things from the quantum world to do calculations with information. The aim is to create ways of solving problems much faster than regular computers can. This paper will explain why we need quantum computing and what benefits it brings compared to regular computers. We'll also talk about the important parts of quantum computing and the difficulties it faces.

Key words: Quantum, Information processing, Quantum computer, Qubits, Classical computers

1. INTRODUCTION

Quantum computing is a new and exciting field that deals with computers different from the regular ones we use every day. These computers, called quantum computers, work using tiny particles like atoms and electrons. These tiny particles behave in ways that are really different from the things we see in our everyday world. Regular computers use bits, which are like tiny switches that can be either 0 or 1. But in quantum computers, these tiny particles, called quantum bits or qubits, can be both 0 and 1 at the same time! This special ability makes quantum computers very powerful for solving certain types of problems.

Scientists are working hard to build quantum computers because they might be much faster than the computers we have now. They could help us solve some really tricky problems that are too hard for regular computers to solve quickly. However, building and using these quantum computers is really tricky too, and there's still a lot we need to learn about how they work.

2. Quantum Computing

Quantum computers are special because they use a different calculation method than regular computers. Regular computers, like the ones you use daily, work using tiny switches called transistors. But quantum computers are based on a principle called superposition, which is a special thing in the science of very small particles called quantum mechanics.

Regular computers use "bits" that can be either 1 or 0 to store and process information. Quantum computers use "qubits," which are like supercharged bits. These qubits can be in a state called superposition, meaning they can be both 1 and 0 at the same time. This is different from regular computers.

There's something called a quantum Turing machine, which is like the main idea of a powerful quantum computer. It's a theoretical model, a way of thinking about how these computers might work. Quantum computers also have some things in common with special kinds of computer programs that use randomness and probability to solve problems.

2.1 Basic of Quantum computing:

A classical computer is not as good as a quantum computer because it's slower at solving some types of problems. Usually, we'll change a regular computer to make a quantum computer. This new computer will have a special setup called a "quantum circuit" added to it. Also, there will be a way for the regular part of the computer to connect and work together with this new quantum part.

Bits and Qubits:

A qubit is the fundamental unit of information, analogous to a classical bit in classical computing. However, unlike classical bits, which can exist in a state of either 0 or 1 at any given time, qubits can exist in multiple states simultaneously due to a property called superposition.

This superposition property allows qubits to represent and store much more information than classical bits.

While a classical bit can only be in one state at a time (either 0 or 1), a qubit can exist in a combination of 0 and 1 states simultaneously. This unique characteristic enables quantum computers to perform certain types of calculations much more efficiently than classical computers.

Qubits have another property called entanglement. When qubits become entangled, the state of one qubit becomes interconnected with the state of another, even if they are physically separated by a great distance. This phenomenon enables quantum computers to perform complex operations and computations that classical computers would struggle with.

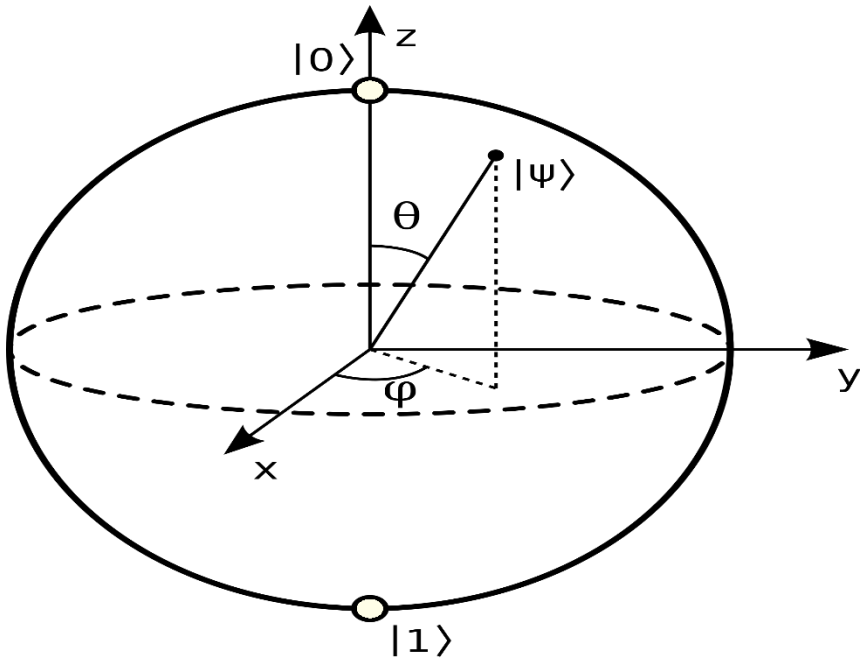
Qubits form the basis of quantum computing and their ability to exist in superposition and entangled states is what gives quantum computers their potential for solving certain problems more efficiently than classical computers.

Superposition state:

Superposition occurs when the qubit exists in a combination of $|0\rangle$ and $|1\rangle$ states simultaneously. Visually, this can be depicted as a point on the surface of the Bloch sphere

that is not at either |0⟩ or |1⟩ but rather somewhere in between. Imagine the qubit's state being in a location that isn't at the poles (|0⟩ or |1⟩), but rather on the sphere, representing a mix of both states.

Qubit can exist in a superposition of two states, conventionally represented as |0⟩ and |1⟩, similar to the classical bits in a regular computer.



Entangled States;

Quantum entanglement is when tiny particles, like those in the quantum world, get connected to each other. When this happens, you can't think about the state of one particle by itself. Instead, the behaviour of one particle depends on the behaviour of another particle that's entangled with it. It's like they're dancing together, and what one does affects the other, making them act as a team even if they're far apart.

Subatomic particles sometimes get into a special connection called "entanglement. "When these particles are entangled, if something happens to one of them, the other particle immediately feels it, even if they're really far away from each other.
$|\Phi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$

Quantum gates;

Single Qubit Gates: These gates are like instructions or rules that we use to change the state of a qubit. They perform various operations on the qubit's state to manipulate or transform it.

They perform various operations on the qubit's state to manipulate or transform it.

(a) NOT Gate (X Gate): This gate is similar to flipping a coin from heads to tails or vice versa. When applied to a qubit in the |0⟩ state, it changes it to the |1⟩ state, and when applied to a qubit in the |1⟩ state, it changes it to the |0⟩ state.

The matrix X representing the quantum NOT gate is then defined as follows:

$$x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

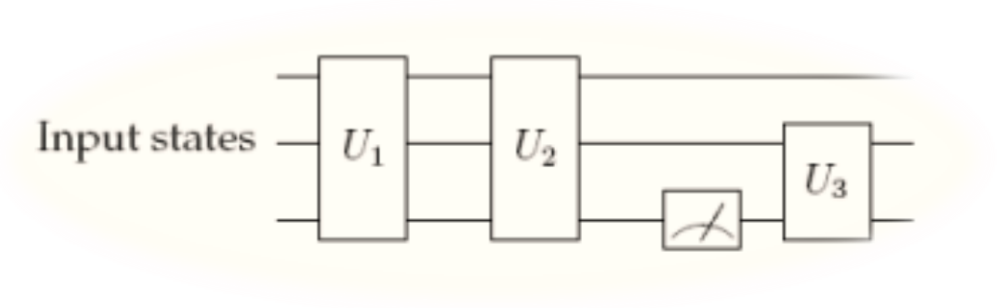
(b) Hadamard Gate (H Gate): This gate is like a mix or blend operation. It puts the qubit into a superposition state, meaning it can be in both |0⟩ and |1⟩ states simultaneously, with specific probabilities for each state when measured.

$$H = 1/\sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Quantum Circuits:

Quantum circuits represent a sequence of quantum operations that transform the initial state of qubits. Quantum circuits operate in a way that's analogous to classical circuits. They usually end with a measurement operation.

When the qubits are measured, their quantum superposition states collapse to classical states (0 or 1), providing the final outcome of the computation.



3. QUANTUM COMPUTER

Quantum computers utilize the principles of quantum mechanics to perform computations, offering the potential to solve certain problems significantly faster than classical computers.

Quantum computation aims to harness the unique properties of quantum mechanics to perform computations that are beyond the capabilities of classical computers. It's important to note that while quantum computers offer immense potential for solving specific problems faster, they are not intended to replace classical computers entirely. Instead, they are seen as powerful tools for solving certain classes of problems that are intractable or extremely time-consuming for classical computers.

Currently, practical quantum computers are still in their early stages of development, facing challenges such as maintaining qubit stability, error correction, and reducing the effects of decoherence. Researchers and companies worldwide are actively working on advancing quantum computing technology to unlock its full potential for various applications in fields like cryptography, drug discovery, optimization, and more.

Quantum Algorithms: Algorithms specifically designed for quantum computers, like Shor's algorithm and Grover's algorithm, take advantage of quantum properties to solve certain problems more efficiently than classical algorithms. For instance, Shor's algorithm offers a quantum advantage in factoring large numbers, which is crucial for cryptography.

Quantum algorithms, such as Shor's algorithm and Grover's algorithm, provide substantial speed-ups for specific problems. Shor's algorithm, for instance, can efficiently factor large numbers, which is a problem that classical computers struggle with due to its exponential time complexity.

As quantum computing technology advances and matures, it's expected that quantum computers will unlock new possibilities and applications, contributing to a broader spectrum of problem-solving across various fields of science, technology, and industry.

3.1 Types of Quantum Computer

- **Quantum Annealer** -The quantum annealer is least powerful and most restrictive form of quantum computers. It is easiest to build yet can only perform one specific function. The consensus of the scientific community is that a quantum annealer has no known advantages over conventional computing.

- **Analog Quantum-** The Analog quantum computer will be able to stimulate complex quantum interactions that are intractable for any known conventional machine or combinations of these machines.

4. CHALLENGES

Building a quantum computer is really tough and main types of challenges:

The physics challenges are mostly about how long the bits (called qubits) can stay in their special states without losing their information. Qubits need to stay in a 'superposition' or 'entangled' state without getting messed up. Scientists also need to find ways to make qubits more exact and fix any mistakes that happen when doing quantum operations. For the engineering part, the big challenge is making these quantum computers bigger. To do anything useful, we might need loads and loads of qubits. But because of the tricky physics stuff we talked about earlier, it's tough to make a bunch of qubits work together perfectly.

5. CONCLUSION

Quantum computing and quantum technology have been in the news for some time. The scientists know that it' an exciting area. For the past five to ten years, many folks thought that the progress in this field was way ahead in the future. They believed it would be a long time before we could build machines that could actually do useful stuff using quantum principles. That's because quantum mechanics, which is the science behind quantum computing, is quite complex and hard to control. People thought it would take ages to figure out how to make machines that could use these weird quantum rules to do anything practical.

Progress in quantum technology has been moving faster than expected. Scientists and engineers have been making breakthroughs in understanding and controlling quantum systems. Quantum computers, although still in their early stages, are showing promising signs of becoming practical and useful for solving real-world problems.

REFERENCES

1. Nielsen, M., and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2000).
2. Aaronson, Scott, and Dave Bacon. "Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment." Computing Community Consortium, and Version 6 (2008).
3. Quantum Computing: A Short Course from Theory to Experiment, by Joachim Stolze, Dieter Suter, Wiley publications
4. Bennett, C. H., DiVincenzo, D. P., Smolin, J. & Witter's, W. K. Mixed state entanglement and quantum error correction. Phys. Rev. A 54, 3824–3851 (1996).
5. D. P. DiVincenzo. Quantum computation. Science, 270:255
6. C. Zalka. Simulating quantum systems on a quantum computer. Proc. R. Soc. London A, 454(1969):313–322, 1998
7. Terral, B. M. Quantum Algorithms and Quantum Entanglement. Thesis, Univ. Amsterdam (1999).
8. Aaronson, Scott. "The limits of quantum computers." Scientific American 298.3 (2008): 62-69.
9. Aaronson, Scott, and Dave Bacon. "Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment." Computing Community Consortium, and Version 6 (2008).
10. Aaronson, Scott. "The limits of quantum computers." Scientific American 298.3 (2008): 62-69.