A Brief Overview of Quantum Computing

Abstract - This mini-dissertation offers a concise overview of quantum computing, beginning with a worked example comparing qubits and binary bits. It explores fundamental quantum principles, including superposition, entanglement, and interference, and examines quantum supremacy with a focus on Shor's algorithm. The paper further investigates the Circuit model of quantum computing and addresses the significant challenges hindering future advancements in the field.

Introduction

A pivotal moment in the history of quantum computing came in 1981 when Richard Feynman stated that classical computers struggled to simulate quantum environments[1]. He then suggested that a computer based on quantum mechanics would be better suited and ultimately superior to this task. The first theoretical model of a quantum computer arrived in 1980 through Paul Benioff [2], where he described a quantum version of Turing machines. David Deutsch advanced this concept in 1985 [3], generalizing to a universal quantum computer and providing the framework for quantum gates and algorithms, an essential component for any computer.

Qubits vs. Classical Bits

The operation of all computers builds off a fundamental unit of information. Classical computers use a binary digit (bit) set to 0 or 1, often imagined as a switch that can be only on or off. Quantum computers use Qubits; these qubits can exist in a superposition of 0 and 1 and collapse down to a definite state when observed. Felix Bloch visualised them through a Bloch Sphere [4], A 3-D sphere containing an arrow that represents the qubit's current state, the top of the sphere is defined as 1. In quantum physics, we define qubits as a state represented by a wavefunction:

$$(|\psi\rangle = \alpha|0\rangle + \beta|1\rangle) \tag{1}$$

The fundamental difference between classical and quantum computers lies in the use of qubits, which can exist in superposition states. We will now explore a 3-bit/qubit state for a classical and quantum computer to demonstrate this:

Classical - 3 bits form a bit string of: `[000, 001, 010, 100, 011, 110, 101, 111]`
Classical computers can be in only one of these states: **Number of states = 1**

Quantum - 3 qubits, entangled, form a quantum register described by the following equation:

$$\frac{1}{\sqrt{8}}\left((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)\right) \equiv \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right) \tag{2}$$

This equation is a superposition of all eight state vectors possible. Here, the Quantum computer can be in all states simultaneously, giving rise to the equation: **Number of states = $\mathbf{2^N}$**, where N is the number of qubits. This difference in the number of possible states at a time gives rise to the exponential advantage of quantum computers.

Underlying Quantum Principles

Superposition - The ability to exist in multiple states simultaneously is called superposition, and it is used here to explain qubit states; this property is what ultimately allows the quantum computer to perform many calculations at once.[5]

Entanglement - Refers to the ability for individual qubits to become part of a larger quantum state where measurements or manipulation on one qubit, affects the other qubits instantaneously. This is the principle that gives quantum computers the exponential edge over classical computers.[6]

Interference - Qubits are mathematically represented as wave functions (1). Entangling qubits combine their wave functions, causing constructive and destructive interference. Quantum algorithms use constructive interference to increase the probability of the correct answer and destructive interference to decrease the probability of the wrong answer in the total entangled quantum state.[7]

Quantum Supremacy

Quantum supremacy is achieved when quantum computers outperform classical ones on a specific task. An example occurred in 2019 when a quantum computer completed a task in 200 seconds that its creators claimed would take 10,000 years on a classical computer [8] (this was later corrected to 2.5 days on the fastest supercomputer)

Quantum computers achieve remarkable speed through using quantum algorithms, that only work on quantum systems. One such algorithm, **Shor's Algorithm** [9], focuses on the factorization of large numbers. While classical computers scale the problem as $2^{\frac{N}{2}}$ (where N is the length of the number), quantum computers scale it as $log(N)$, dramatically reducing the time required for large-scale factorization. Here, 'scale' refers to how the difficulty of a problem increases as its numerical size grows.

Quantum computers should continue to surpass their classical counterparts in specific areas, such as quantum simulations (quantum systems, behaviour of exotic materials, chemical reactions, and more), database searching, machine learning, and various other fields. Additionally, there may be unforeseen areas where quantum computers will excel, much like how the full potential of classical computers was unrecognized when they first emerged.

Models

In quantum computing, models refer to theoretical frameworks or conceptual systems for manipulating qubits. They are blueprints for building and analysing quantum computers by defining the operations, algorithms, and rules that control quantum systems.

The most widely used and understood model is the **Circuit or Gate Model** [10]. This model involves a system of qubits, which can be entangled, and quantum gates that perform operations on a small number of qubits. Here, quantum algorithms apply a sequence of gates in a specific order, with a final measurement step to extract the result.

Challenges

Quantum systems are notoriously hard to control, often having to be kept at nearly 0 Kelvin to reduce effects being induced by the outside world. There are three major challenges,

Decoherence: If quantum systems interact with the outside world, they can lose coherence, leading to information loss or corruption. Additionally, it can cause the system to lose its quantum properties, such as superposition, and start to behave classically.

Noise: Electromagnetic waves, cosmic particles, heat, and other factors can similarly affect quantum systems by interfering with qubits and disrupting computations.

Scalability: As quantum systems grow in scale, many issues, including decoherence, become progressively worse. Additionally, the complexity of the physical quantum system increases with the number of qubits, introducing unique engineering challenges.

Conclusion

In conclusion, quantum computers can outperform classical computers in specific tasks by leveraging the quantum properties of superposition, entanglement, and interference through the use of qubits. These properties allow quantum computers to process tasks exponentially faster than classical computers. While there are still tremendous issues to overcome, quantum computing is rapidly transitioning from theoretical concepts to future technology.

References

[1] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, 1981.

[2] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of statistical physics*, 22:563–591, 1980.

[3] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[4] Felix Bloch. Nuclear induction. *Physical review*, 70(7-8):460, 1946.

[5] Paul Adrien Maurice Dirac. *The principles of quantum mechanics.* Number 27. Oxford university press, 1981.

[6] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[7] Richard P Feynman, Albert R Hibbs, and Daniel F Styer. *Quantum mechanics and path integrals.* Courier Corporation, 2010.

[8] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[9] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information.* Cambridge university press, 2010.