ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

An Overview of Quantum Computing's Potential to Solve Complex Problems

Syeda Kawsar

USA

ABSTRACT

Quantum computing is necessary to be described as a powerful tool is the new generation of computational power that works based on the principles of quantum mechanics, allowing the solving of problems that are intractable for classical computers. Due to the utilization of such phenomena as superposition, quantum entanglement and quantum interference, quantum computers are said to be able to solve problems in such areas as cryptography, artificial intelligence, optimization problems and material sciences, among others. This paper attempts to examine the basic concepts of quantum computing while focusing on their different aspects and their potential impacts. This study its experience and potential in its current form and in future applications through examples, illustrations, and theoretical discussion. Specific problems, including error correction, hardware scalability, and requirements for resources to address, make the paper a comprehensive overview of the quantum computing potential and weaknesses. Moving towards practical examples, the discussion covers all aspects of the book, providing readers with a holistic understanding of how quantum computing is going to change technological paradigms in the forthcoming decades.

***Corresponding author**

Syeda Kawsar, USA.

Received: December 06, 2022; **Accepted:** December 14, 2022, **Published:** December 28, 2022

Keywords: Quantum Computing, Qubit, Cryptography, Optimization, Quantum Algorithm, Superposition, Entanglement, Grover's Algorithms, Shor's Algorithms

Introduction

The growth of classical computing follows an exponential curve defined by Moore's Law, yet its growth is soon to be limited by the physical world's inability to reduce the size of the transistor and improve its energy efficiency. Quantum computing is a revolutionary idea as classical systems approach these limitations at the edge. Quantum computing, on the other hand, works differently from classical computers in that it uses quantum bits or qubits that can be in more than one state at the same time [1]. Here, it is talking about the principle called superposition; combining this with entanglement and interference is what makes a quantum computer capable of performing calculations that could be impossible for a classical computer.

This paper seeks to establish the basic principles of quantum computing and quantum computing across main spheres. Quantum computing prospect is breath-taking; it can both break cryptographic protocols, optimize complex systems, and enhance artificial intelligence. But the paper also looks at the technical and operational hurdles that need to be crossed to fully unlock its potential. It thereby sets out a starting point to help map the nature of change that this, at present pioneering, technology can offer.

Fundamentals of Quantum Computing

Quantum computing differs significantly from classical computing as classical computing relies on the physics of recipes, and quantum computing relies on the physics of recipes. More fundamentally, quantum computing involves the use of qubits, which, unlike more conventional binary bits, exist in a binary state of either 0 or 1; or both.

Key Features

Superposition: Qubits can exist in phase space analogous to being in two states at the same time as the classical bits that are either 0 or 1. In mathematics, a qubit is described by a linear combo of the two basis states, for example, $\alpha|0> + \beta|1>$ where α and β are mentioned as probabilities of measurement of the qubit in that particular state.

Entanglement: Quantum computers can be linked or made to share information between qubits wherever they are located. The value '1' of this property allows for extremely parallel operation
Quantum Interference: Interference enables quantum algorithms to strengthen the probability of correct solutions and cancel the incorrect ones, thereby making computation faster.

Quantum Gates and Circuits

Quantum operations are made through quantum gates that act on qubits. These gates include:

- **Hadamard Gate:** Gives superposition for every state of a system by partitioning equal probability at 0 and 1.
- **CNOT Gate:** Obtained by linking the state of two qubits such that the state of one will influence the other [4].
- **Pauli Gates (X, Y, Z):** Make rotations around the X, Y and Z axes of the Bloch sphere.
- These gates are implemented in a quantum circuit that are used to perform certain computations. For instance, a basic quantum algorithm could be applied, such as a Hadamard gate to place the qubits into a superposition, a CNOT gate to place the qubits into entanglement, and measurement to extract the raw results.

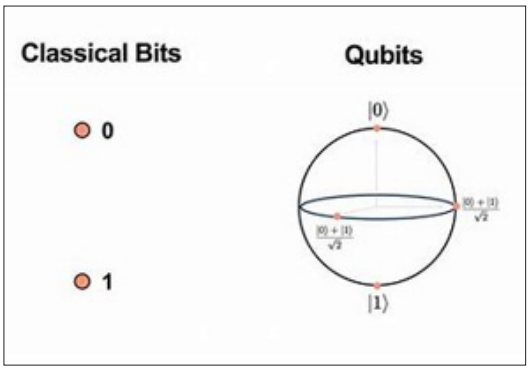

Figure 1: Classical Bits and Qubits [2].

Quantum Algorithms

The strength of quantum molecular computing is not in the computational power of quantum computers but in their algorithms based on quantum realities.

Shor's Algorithm

Shor's algorithm is the polynomial time algorithm that solves one of the most essential problems for cryptography – integer factorization. Standard methods for factorization are exponential thus not efficient to be used in large numbers.

Pseudocode for Shor's Algorithm:
Input: Composite number N.
Step 1: Choose a random integer a < N
Step 2: Compute gcd(a, N). If gcd ≠ 1, return gcd.
Step 3: Use quantum Fourier transform to find period r of a^x mod N.
Step 4: Compute factors as gcd(a^{r/2} - 1, N) and gcd(a^{r/2} + 1, N).

Grover's Algorithm

It has to be noted that Grover's algorithm offers quadratic speed up in case of unstructured search situations. Classical algorithms in fact need queries to search for a given item in an unordered database of size, but Grover's algorithm only needs queries.

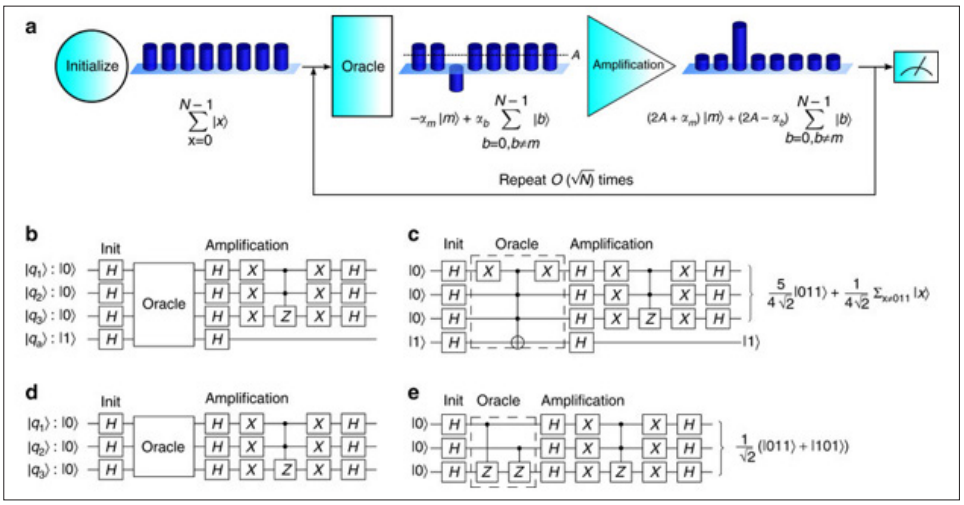

Figure 2: Grover Search Algorithm [3].

Uses of Quantum Computing

Cryptography

Despite those long established by quantum computing, there are both threats and opportunities in cryptocurrency. Candidates like Shor are capable of discrediting conventional encryption strategies, including RSA and ECC, through efficient factoring of numbers. Similarly, post-quantum algorithms, including the lattice algorithms, are being devised to handle these risks.

Optimization Problems

Optimisation is the other area in which quantum computing is a gem. For instance, the Quantum Approximate Optimization Algorithm (QAOA) solves combinatorial optimization issues that appear in logistics, finance, and scheduling [4]. For example, QAOA can solve the problem of supply chain logistics paths and do so much faster than a classical computer.

Artificial Intelligence

Quantum Machine Learning (QML) improves classical skills of Artificial intelligence by slicing and dicing big data exponentially. Some examples, such as quantum machine learning (QML), reveals how this field can advance artificial intelligence: It highlight quantum support vector machines, neural networks, and clustering algorithms.

Specially Material Science and Drug Discovery

They are best suited to the analysis of other quantum systems, for example, in the design of new materials and in pharmaceuticals. For instance, predicting, for example, the manner in which large molecules like proteins behave helps to quicken the process of developing drugs.

Climate Modeling

Currently, quantum algorithms suggest an approach to simulate other climate systems to make better predictions of Global warming situations.

Case Studies

Logistics Optimization

A logistics problem in the context of the supply chain management, namely the problem of determining the optimal routes for a number of delivery vehicles, shows the benefits of quantum computing. Classical algorithms, on the other hand, tend to be slow and face issues of scalability while QAOA indeed brings near-optimal solutions.

Drug Discovery

Typically, a coarse-grained simulation of a protein's interaction

with a potential drug candidate has been a prohibitively computationally intensive task. Quantum simulations limit these requirements and longstanding cycles for drug creation.

Challenges and Limitations

Despite its promise, quantum computing faces significant obstacles:

- **Error Correction:** Quantum systems are mainly characterized by decoherence and noise [5]. Method like the surface code maps a logical qubit ontologically so as to be error correcting.
- **Scalability:** It is a significant engineering task to construct scale-up systems that can incorporate millions of immune-to-error qubits. Pertaining to the current state of affairs the number of qubits is usually kept below 100 by most quantum computers.
- **Software Development:** Quantum programming is special and cannot be very accessible to most programmers in the market.

Roadmap to Quantum Advantage

The path to practical quantum computing involves three milestones:

- **Noisy Intermediate-Scale Quantum (NISQ) Era:** Solvers that nowadays can only tackle problems of modest size with a number of qubits [6].
- **Fault-Tolerant Quantum Computing:** Machines that can, therefore, compute error-free for long periods are called systems.
- **Quantum Supremacy:** Realizing Problem Solving that classical computers are incapable of solving.

Conclusion

Quantum computation can show revolutionary applications in pretty much every subject, spanning from cryptography, optimization, artificial intelligence, and material science to climate computations. While at present, the error correction, scalability, or the demand for huge resources can be a problem with the existing implementations, the current development of the hardware and algorithms are opening up realistic prospects for their integration. It is presumed that with increasing cooperation between academia, industry, and government, these barriers will be dispelled, fully unlocking the capability of quantum computation.

Quantum technology is a young science, but its future is traced. It is only now that it see great potential in the realization of ideas viewed as fantastic yesterday. And yet, it is quietly and steadily moving from the laboratories into practical applications where the impact is expected to be revolutionary in the worlds of science, technology and society. Quantum communication demands the reconsideration of the approaches to problem-solving and offers directions previously unavailable for development. In addition, the ability of quantum computing to accelerate disruption in different industries is evident in the impacts it creates in the present and fosters in the future. In cryptology, safe-guarded digital communications by the development of quantum-resistant algorithms will be ready, but in Artificial Intelligence, quantum-assisted models for data analysis and decision-making will likely be revolutionary. In material sciences and drug design, quantum simulations provide close to perfect accuracy and speed up the rate at which new technologies and cures are created.

References

1. Cao Y, Romero J, Aspuru-Guzik A (2018) Potential of quantum computing for drug discovery. IBM Journal of Research and Development 62: 6: 1-6.
2. (2020) Quantum Computing Explained: Will it replace our PCs? [online] Tech Centurion. Available at: https://www.techcenturion.com/quantum-computing/.
3. Figgatt C, Maslov D, Landsman KA, Linke NM, Debnath S, et al. (2017) Complete 3-Qubit Grover search on a programmable quantum computer. Nature Communications 8.
4. Bravyi S, Dial O, Gambetta JM, Gil D, Nazario Z (2022) The future of quantum computing with superconducting qubits. Journal of Applied Physics 132: 160902.
5. Bhat HA, Khanday FA, Kaushik BK, Bashir F, Shah KA (2022) Quantum Computing: Fundamentals, Implementations and Applications. IEEE Open Journal of Nanotechnology 3: 61-77.
6. Coccia M (2022) Technological trajectories in quantum computing to design a quantum ecosystem for industrial change. Technology Analysis & Strategic Management 1-16.