Solving Classical Computing Problems Via Quantum Computing

David Wisnosky, School of Computing, University of North Florida

Computing Paradigms

Classical Computing

The field of computing is founded upon the abstraction of math and physics.

The father of computing Alan Turing developed a mathematical model for today's modern computers. This model is known as the **Turing Machine**. This model provides a mathematical way of determining if problems are solvable by a computer.

Computers are **deterministic**. Meaning, that the outcome of a computation is determined exclusively by the previous steps.

This model for computation is defined as **classical computing**. Due, its limitations certain computational problems currently exist.

Quantum Computing

A young sub-discipline of computing known as **quantum computing** has become increasingly popular, as it aims to solve the problems of Classical Computation.

Like classical computing, quantum computing is modeled using math and physics. With its own models as well, the **Quantum Turing Machine** and the **Quantum Circuit Model**.

Quantum computers take advantage of the unpredictable nature of quantum physics and exploit this to aid in the speed and capability of computations.

A Quantum computer operates on three major postulates, they are as follows:
Superposition: The idea that a quantum state exists in a combination of the base states.
Entanglement: A state in which two quantum states are intrinsically linked.
Measurement: The act of preforming an observation on a quantum state.

By using these principles one can solve many problems currently impossible or infeasible by a classical computer.

Mathematical and Scientific Foundation

Classical Computing

- Operations based on Boolean algebra.
- Implemented via principles of electricity.
- Base unit is the binary digit or **bit** either a 0 or 1. Can be viewed as either heads or tails.
- Bits form the state of a computer. Where the state refers to the information it stores, at a given time. Classical states store information equivalent to the number of bits that comprise the state. n bits provide n bits of information.

Quantum Computing

- Operations on linear algebra.
- Implemented via principles of quantum physics.
- Base unit is a quantum bit or **qubit** exits as a combination of either a 0 or 1. Can be viewed as a rolling coin. With some probability of heads or tails at a given moment.
- Qubits form a quantum state and store information equivalent to 2^n classical bits.

Classical Computing Problems

High Computational Complexity: Certain problems have many possible solutions, often there are so many that a computer without an efficient way to solve such a problem, cannot compute all options in a reasonable time.

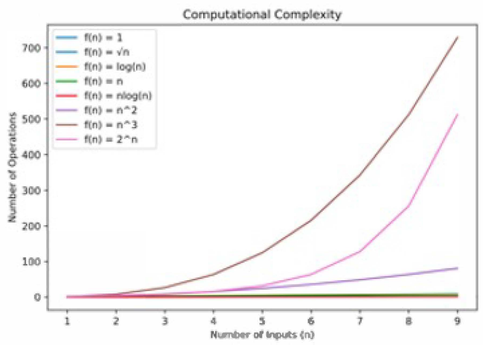

Fig. 1 Common complexity functions

Random Number Generation: Classical computers cannot produce genuinely random numbers; they instead take a changing value such as the date and scramble it. However, given the same input, the seemingly random output will be identical.

Reversibility: Classical computation often cannot be reversed, meaning one cannot retrieve the inputs from the outputs.

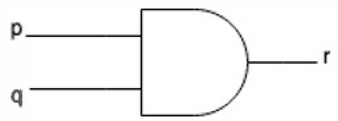

Fig. 2 Non-Reversible Circuit (AND Gate)

Conclusion

The goal of quantum computing is not to upend the way the world uses computers. First, the materials and devices needed to create a quantum computer are rare and inordinately expensive. Second the tasks most people do on their computers would receive no benefit from a quantum computer. Not mention that these devices are very inaccessible. One way one can use a quantum computer is via IBM's Qiskit, but this requires prior knowledge of both the quantum and classical computing paradigms.

Quantum computers are still computers and thus follow what is known as the **Church-Turing thesis**, which defines what is theoretically computable. Simply put this means that a quantum computer and classical computer can do the same things, only one may do so faster.

Given current research there is still no guarantee that quantum computers are faster. In 2019 Google claimed **Quantum Supremacy**, but this claim was considered overblown by experts and competitors.

What can be said however, is that quantum computing solves many issues currently faced by the computing community today. As computers are no longer getting exponentially faster a new approach must be taken. Currently this approach has manifested itself in the form of quantum computing and is a promising field.

References & Acknowledgements
[1] *Quantum Computing: A Gentle Introduction*. (2011). MIT Press.
[2] Sipser, M. (2013). *Introduction to the theory of computation*. Australia: Course Technology Cengage Learning.
[3] *Qiskit* (0.24.1). (2021). [Quantum Computing API]. IMB. https://qiskit.org/
Dr. Asai Asaithambi, Professor and Graduate Director, School of Computing, University of North Florida

Quantum Computing Solutions

Computational Complexity: Due to the principle of superposition, a qubit stores more information than a classical bit. This can be used to perform more calculations simultaneously when compared to a standard computer. An example of this speed-up is Grover's algorithm for searching a database. Normally when searching a database for a particular entry one would need to search at most all n entries. This is what a classical computer does, and this search is known as linear time search as the time taken grows directly proportional to n. Grover's algorithm utilizing a quantum computer performs the same task in time proportional to √n this is a significant speed increase.

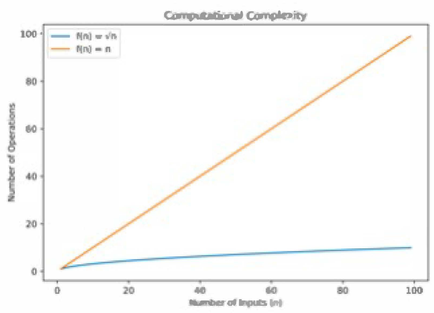

Fig. 3 Complexity of linear search vs Grover's algorithm

Random Number Generation: Another aspect of quantum physics that can be utilized for computation is the truly random nature of particles. It is these particles that form the basis for quantum physics and therefore quantum computing. Using these random particles random computation can be achieved.

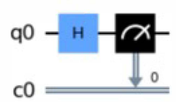

Fig. 4 A quantum circuit for generating a 0 or 1 randomly.

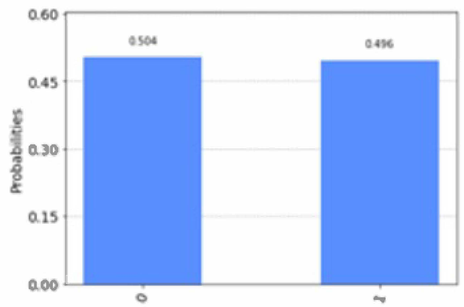

Fig. 5 Probabilities of the state collapsing to a 0 or 1. Run on a real quantum computer.

Reversibility: Another fundamental aspect of quantum computing is that all its operators allow for reversible computation. Meaning the inputs can be retrieved from the outputs. The quantum circuit model also demonstrates this.

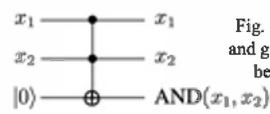

Fig. 6 A quantum and gate where can be retrieved.