Kenrick Lam, 301357041

James Northway, 301303312

Steven Tran, 301303981

Steven Le, 301273157

Jograj Sidhu, 30133182

CMPT 409 assignment 1

Introduction

In classical computing, data is represented as a series of 0s and 1s which are known as bits. A single classical bit can either be a 0 or it can be a 1, but it cannot be both at the same time. This makes sense as pieces of information are simply a tuned series of 0s and 1s that make up its representation in machine (binary) code. If a single bit is switched to its counterpart, for example switching a 0 to a 1, then that information can be vastly different from the other. In quantum computing, bits are not fixed and have a different nature. A quantum bit, also known as a qubit, can be either a 0 or a 1 or both at the same time. This nature of simultaneously being both states at the same time is known as superposition and is quite common in quantum computing. Clever algorithms can exponentially speed up certain problems, by use of destructive interference and constructive interference to cancel incorrect computational paths and increase the probability of correct answers respectively (Aaronson, 2008, 62-69). It is one of the reasons why quantum computers can perform certain classical algorithms exponentially faster than a regular computer, as qubits in superposition can represent 2n states as opposed to n2 - 1 states of classical bits. Figure 1 below gives a visualization of how to interpret a quantum bit relative to a classical computing bit (Dumon, 2019).

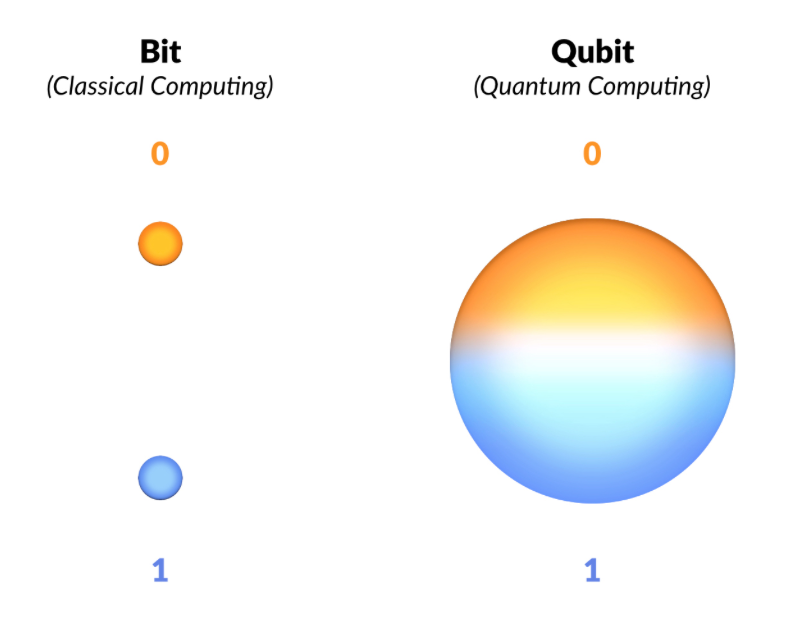


Figure 1: Here, you can see that a quantum bit is a linear combination of the two states, 0 and 1, and while in superposition, is in two states at the same time.

Also of note is quantum entanglement, which is the phenomenon where the state of each particle within an entangled group will share information of the other particle's state when observed, regardless of distance. No matter how far apart the particles are from each other, their final states will be directly correlated. Through clever manipulation of an entangled group of qubits using quantum logic gates, one can lead qubits towards the desired correct answer. This is due to the ability for events with positive and negative amplitudes to be cancelled out during the runtime of a quantum program. By actively cancelling paths that lead to incorrect answers, a quantum computer can coerce the qubits to collapse into the correct state when observed.

Two maximally entangled qubits

One possible explanation for this phenomenon is a so-called hidden variable. In this interpretation, entangled particles have an unknown property that allows them to predetermine their outcome during the entanglement before any measurement of the pair occurs. However, when calculating the correlation measures between these particles, they have a predicted correlation value of 22, and not the expected maximum value of 2 if using reasoning based on the hidden variable theory. This suggests there are quantum mechanics involved.

The four states of a qubit pair that leads to this maximal value of 22 are known as the four maximally entangled two-qubit states, or the Bell states. Measuring one of the entangled pair yields consistent results in the second qubit, being either the same value as the first qubit if they are in one of the 𝜱 states or the opposite value if they are in one of the 𝛹 states. This property is the basis of quantum computing and quantum information theory.

Applications

One major application of quantum computing is in the field of breaking cryptographic keys. Currently, many of the encryption methods used rely heavily on the near impossibility of conventional computers determining the factors of a number that is the product of two extremely large prime numbers. A popular encryption technique, known as RSA, now typically produces a number that is 617 digits long (Lake, 2021), which is big enough of a number that it is essentially pointless to try brute-forcing its two factors. However, quantum factoring algorithms could make this no longer the case. Quantum algorithms such as Shor’s Algorithm can be used to factor integers in polynomial time (Qiskit, n.d.). However, current applications are still very limited due to the difficulty of manipulating qubits; as of now the record for the largest number factored using Shor’s algorithm is 21, set in 2012 (Martin-Lopez et al., 2012, 1).

Another application of quantum computing is its ability to heavily reduce the runtime of search algorithms. Many conventional search algorithms such as the O(logn) binary search requires that the list being searched is sorted. However, Grover’s algorithm can search for an item in an unsorted list in O(n) steps. Grover’s algorithm can also be used to dramatically increase the runtime of other algorithms due to a property called the amplitude amplification trick (Qiskit, 2021).

Limitations

Theoretical limitations exist in our universe. Einstein’s theory of relativity explains that the laws of physics apply to all objects regardless of their frame of reference. This statement proves that the speed of light is the same no matter the reference frame and thus no object may travel faster than the speed of light (Norton, 2013). Yet as explained above, observing the value of an entangled qubit can instantaneously result in information about the entangled counterpart’s state to be known regardless of the distance between the two qubits. This phenomenon has been famously dubbed by Einstein as “spooky action at a distance” since at first glance, it seems to suggest the possibility of superluminal communication. However, this does not allow us to transmit information. Suppose we have two entangled qubits at two infinitely separated locations, the fact is that if we force the qubit at location 1 into a particular state then observe the qubit at location 2, we will see that the results are uncorrelated. This is because forcing a quantum particle into a state will break any entanglement that it has. This limitation of quantum physics makes superluminal communication impossible (Siegel, 2020). So even though quantum physics allows for violating the principle of locality, it is still limited by the laws of physics and cannot perform superluminal communication.

Another important theorem to consider is the no-communication theorem which essentially states that it is impossible to transfer classical bits of information using shared quantum states (Wikipedia, 2021). This theorem is significant because it implies that superluminal communication is impossible using quantum entanglement since that phenomenon relies on shared quantum states. The proof of the no-communication theorem starts by describing two observers, Alice, and Bob, each having their own spatially distinct portion, A and B respectively, of some quantum state. It is also assumed that the total state of A can be described by some density matrix 𝝈 and that by measuring the quantum state via performing some projection P on the matrix, it would then collapse into the state P(𝝈). The proof concludes by showing mathematically that the trace of the matrices 𝝈 and P(𝝈) are equal which implies that Bob would not be able to tell whether Alice measured her quantum state or not. As a reminder, the principle of locality states that an object is directly influenced only by its surroundings and that all such influences are limited by the speed of light as mentioned earlier above. However, the no-communication theorem shows that even if the principle of locality is violated, superluminal communication via quantum entanglement is impossible. Since there is nothing that one observer can do to one entangled particle that would be detectable by another observer with the other entangled particle, no new information would be shared between the two.

References

Aaronson, S. (2008, March). The Limits of Quantum. *SCIENTIFIC AMERICAN*. https://www.cs.virginia.edu/~robins/The\_Limits\_of\_Quantum\_Computers.pdf

Dumon, K. (2019, April 16). *The computational power of Quantum Computers: an intuitive guide*. Medium. Retrieved June 4, 2021, from https://medium.com/@kareldumon/the-computational-power-of-quantum-computers-an-intuitive-guide-9f788d1492b6

Lake, J. (2021, March 18). *What is RSA encryption and how does it work?* comparitech. Retrieved June 6, 2021, from

https://www.comparitech.com/blog/information-security/rsa-encryption/

Martin-Lopez, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., & O'Brien, J. L. (2012, October 24). Experimental realisation of Shor’s quantum factoring algorithm using qubit recycling. *Nature Photonics*, (6), 773-776. 10.1038/nphoton.2012.259

Norton, J. D. (2013, February 10). *Special Relativity Principles*. University of Pittsburgh. Retrieved June 12, 2021, from http://www.pitt.edu/~jdnorton/teaching/HPS\_0410/chapters/Special\_relativity\_principles

Qiskit. (n.d.). *Grover's Algorithm*. Qiskit. Retrieved June 6, 2021, from

https://qiskit.org/textbook/ch-algorithms/grover.html

Qiskit. (n.d.). *Shor's Algorithm*. Qiskit. Retrieved June 2021, 6, from

https://qiskit.org/textbook/ch-algorithms/shor.html

Siegel, E. (2020, January 2). *No, We Still Can't Use Quantum Entanglement To Communicate Faster Than Light*. Forbes. Retrieved June 12, 2021, from www.forbes.com/sites/startswithabang/2020/01/02/no-we-still-cant-use-quantum-entanglement-to-communicate-faster-than-light

Wikipedia. (n.d.). *No-communication theorem.* Wikipedia. Retrieved June 12, 2021, from

https://en.wikipedia.org/wiki/No-communication\_theorem