Quantum Computing

Anishka Jannu

August 2024

Quantum computers allow for computations that cannot be done with classical computers. Today's classical computers struggle with excessive searching queries, creating secure encryptions, and simulating quantum mechanics. Quantum computers, on the other hand, are well-versed in large searches, factorizing large numbers into their prime factorizations, quantum simulation, graph theory, and machine learning. The quantum realm allows algorithms to be in quantum parallelism, allowing them to test multiple potential solutions at once, therefore expediting the algorithm. Quantum algorithms can be used to solve complex optimization problems, which was not possible using classical computers.

1 Introduction

While classical computers use classical bits to store information, quantum computers use quantum bits. Also known as qubits, these particles have the ability to exist in multiple states at one time, which we call superposition. Superpositions can be viewed as a linear combination of quantum states, which are represented by vectors. Superposition forms the basis of many of the advantages of quantum algorithms, but it also has its challenges.

A quantum state can be described as a complex direction (vector) in an abstract space:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } \alpha, \beta \in C \text{ and } |\alpha|^2 + |\beta|^2 = 1.$$

While classical bits must be 0 or 1, qubits can be present in any state between 0 and 1. When these particles go through a measurement in order to learn more about the information they hold, they give up their superpositions and randomly choose a single state. Because measuring qubits destroys their superposition, we are unable to gain much information about the original state of the particle. In addition, measurement results in an output of 0 or 1, which does not preserve the complicated states that the qubits exist it. Decoherence, which results in the loss of quantum properties when quantum systems interact with external environments, causes quantum systems to have a limited complexity in terms of computation. We can use logic gates and quantum properties to manipulate the information in qubits to use it to our advantage.

1.1 No-Cloning Theorem

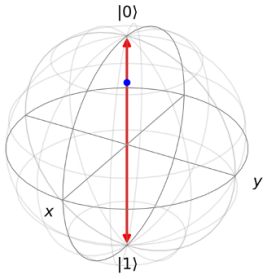
The No-Cloning Theorem states that a quantum state cannot be copied. This is because we are unable to receive all of the information a qubit holds when we measure it, since measurement destroys the original quantum state and forces the qubit to choose a state. One way to attempt to prevent this phenomenon is to use quantum error correction, which allows for the detection and correction of errors in quantum information without actually changing the information, therefore preventing the destruction of the quantum states.

1.2 Logic Gates

Logic gates can be used to manipulate the information that qubits hold. Essentially, logic gates are matrices that are multiplied by the qubits when the gate acts on a state.

Pauli-X Gate

The X-gate, also known as the Pauli-X gate, flips the value of the input between 0 and 1. If we visualize the X-gate on a Bloch sphere, we can view it as rotating the vector around the x-axis by π radians.



The X-gate can also be represented as multiplying the qubit by an identity matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Hadamard Gate

The H-gate, or Hadamard gate, is used to create an equal superposition between 0 and 1. Two Hadamard gates that are applied consecutively do not change the value of the qubit because they cancel each other out.

Hadamard gates can be represented by the matrix $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$.

1.3 Deutsch-Jozsa Algorithm

One famous quantum algorithm is used to determine whether a Boolean function is constant or balanced. A function is constant if it constantly outputs a 0, or a 1. If the outputted values are equally split between 0's and 1's, however, we call it a balanced function.

The Deutsch-Jozsa Algorithm takes qubits and organizes them into Hadamard gates, so that the outputs are ideally presented along an equal superposition of 0's and 1's. Then the oracle uses quantum entanglement to determine whether the outputs are constant or balanced, and measures them to read them.

The Deutsch-Jozsa Algorithm allows for this determination to be made in just 1 query, whereas classical algorithms require a minimum of two queries to be successful and 2^{n-1} queries in the worst case scenario. This algorithm, first discovered in 1992, is a great demonstration of how efficient quantum computing can be when using larger numbers. In addition, it was the first quantum algorithm to represent the separation between quantum computing and classical and present a potential for quantum computing to be faster.

Initially, all qubits are in the $|0\rangle$ state, with an additional qubit in the $|1\rangle$ state:

$$|0\rangle^{\otimes n} \otimes |1\rangle$$

Applying the Hadamard gate creates a superposition among the states, so the system becomes:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

where $|x\rangle$ represents all of the possible states that n qubits can represent. Then, the oracle will apply a phase shift to the qubit using entanglement:

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Then we can repeat the application of the Hadamard gate and perform another measurement. If f(x) is balanced or constant, the probability of measuring

$$|0\rangle^{\otimes n}$$

will vary.

2 Quantum Key Distribution

Quantum key distribution protocols allow us to share passwords for communication more securely than classical cryptographic protocols. These QKD protcols are used to solely send a password between parties (not messages). In addition, the quantum methods are used to distribute a *classical* key.

2.1 BB84 QKD Protcol

The protocol starts with Alice receiving a random key: $k_1, k_2, k_3, ...k_n$
Then, Alice randomly apply multiple H gates to certain parts of her key, causing them to be converted from bits to qubits:

$$|k_i\rangle = \begin{cases} |0\rangle & \text{if } k_i = 0 \text{ and the computational gate is chosen,} \\ |1\rangle & \text{if } k_i = 1 \text{ and the computational gate is chosen,} \\ |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{if } k_i = 0 \text{ Hadamard gate applied (superposition),} \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } k_i = 1 \text{ Hadamard gate applied (superposition).} \end{cases}$$

After this, she sends these qubits $|k_i\rangle$ to Bob through a public quantum channel. Bob takes these qubits and randomly applies H gates to some of these qubits.

If Bob applies the Hadamard gate to the qubit, the transformation can be represented as:

$$H|\psi_i\rangle = H\left(\alpha_i|0\rangle + \beta_i|1\rangle\right) = \frac{\alpha_i + \beta_i}{\sqrt{2}}|0\rangle + \frac{\alpha_i - \beta_i}{\sqrt{2}}|1\rangle$$

After applying the Hadamard gate, Bob measures the qubit. The measurement collapses the qubit into either $|0\rangle$ or $|1\rangle$, resulting in a bit k_i' for Bob's key.

If the Hadamard gate is applied:

$$k_i' = \begin{cases} 0 & \text{with probability } \left|\frac{\alpha_i+\beta_i}{\sqrt{2}}\right|^2, \\ 1 & \text{with probability } \left|\frac{\alpha_i-\beta_i}{\sqrt{2}}\right|^2. \end{cases}$$

If the Hadamard gate is not applied, then Bob measures in the computational basis:

$$k_i' = \begin{cases} 0 & \text{with probability } |\alpha_i|^2, \\ 1 & \text{with probability } |\beta_i|^2. \end{cases}$$

Bob repeats this process for all qubits he received, creating his final key using all the bits $k' = k_1', k_2', \ldots, k_n'$.

After this, Alice and Bob enter a public classical channel and compare the H gates they used. When Alice and Bob have the same bit (because they both used the H gate at that part), they will choose to keep that bit in the final key. When they do not both agree on the basis, they will discard those bits.

Finally, Alice and Bob will share a small part of their key over the public channel. Since measurement is destructive, they will know whether Eve was spying on their communication, which will cause them to notice a change in the two keys and give them the option to discard the whole key. If both pieces of their key are similar, then they will assume that no one was intercepting their communication.

In order to have a key of substantial length, Alice and Bob must start with an extensive amount of bits at the beginning because of the massive amount of discarded bits.

2.2 Entanglement-Based QKD

Another version of the BB84 QKD Protocol relies on the entanglement property of qubits, which states that entangled qubits will have the same state before and after measurement. The protocol starts with multiple entangled pairs, typically in the Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

A qubit from each entangled pair is sent to Alice and Bob, respectively. The shared state of the two qubits is given by:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

Then, Alice and Bob randomly choose to apply Hadamard (H) gates to their qubits. The Hadamard gate H transforms the qubit states as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

After applying the Hadamard gates, the combined state of the qubits becomes:

$$|\Psi'\rangle = \frac{1}{2}\left(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B + |+\rangle_A|-\rangle_B + |-\rangle_A|+\rangle_B\right)$$

Alice and Bob then measure their qubits. Since Hadamard gates were applied, the measurement collapses the superposition state of the qubits. Due to the entanglement, their measurement outcomes are perfectly correlated if they used the same gate. For example, if both Alice and Bob measure in the Hadamard gate and Alice obtains $|+\rangle$, Bob will also obtain $|+\rangle$.

Afterwards, Alice and Bob publicly announce which qubits they applied a Hadamard gate to on a classical channel (but they do not share the actual measurement outcomes). They discard the bits when they did not use the same basis for measurement, and keep the remaining bits.

Since their qubits are entangled, the post-measurement state of both qubits is identical. Therefore, Alice and Bob can ensure that they have the same results. They also repeat the process of sharing a part of their key over the public channel to check for eavesdropping by Eve. If the bits that they share are matching, they proceed with using the remaining bits as their shared secret key. If there are discrepancies, then they know that Eve has eavesdropped, and discard the key.

Image References

[1] - qutip.org/docs/4.1/guide/guide-bloch.html