

A Survey in Quantum Computing

Deepansha Singh & Sejal Madan
West Windsor Plainsboro High School South

1. Abstract

As the world progresses in the technological era, quantum computing is clearly becoming a more prominent use of science and math. Specifically, the fields of electrical and computer engineering, computer science, and physics conglomerate to produce new innovation in quantum algorithms. With more efficient algorithms than classical computing, this survey demonstrates the basics of quantum computing as well as recent advancements in arithmetic. The multitude of quantum gates and existing algorithms give rise to the calculator operations of addition, subtraction, multiplication and division. Specifically, we outline the basics of these circuits, theoretically and mathematically. Although a complex field, a classical analogy can be explained to emerge the quantum algorithms that currently exist. The significance of this lies in the applications of quantum computing. Shor's algorithm contributes to cryptography which is vital to the quantum physics field. Quantum involvement in artificial intelligence and machine learning provides the field of computer science with data to advance the connection between robots and human intelligence. Many scientists are experimenting with quantum teleportation, allowing particle transmission to other parts of the world, or even outside of the earth. Another application we explored in this survey includes financial modeling, where quantum algorithms improve efficiency of business. Overall, by summarizing existing research in quantum computing, we provide

an improving practicality of calculator operations and basic knowledge in the various applications throughout the growing field.

2. Introduction

Quantum Computing is one of the next disruptive technologies which will completely change our universe's landscape. This field harnesses several quantum physics principles such as superposition, entanglement, and decoherence to establish a new version of computing with qubits instead of classical bits. It opens up many new possibilities in terms of the speedup in several classical algorithms as well as the variety of real world applications we are discovering. From using Shor's algorithm in quantum cryptography to make messages being transmitted more secure to conducting experiments on a pair of photons where they are successfully entangled in space, quantum computing has a tremendous scope for improving the world around us. While there have been a few surveys in quantum computing published such as [1] which survey the underlying quantum information theory, this review paper is more comprehensive and adaptable to all readers since it starts from a more fundamental level of understanding and then progresses to more advanced content in quantum computing. This review paper on quantum computing is divided into ten main sections. In this paper, we will be providing a summary of the progress made in this field in terms of the knowledge gained, synthesizing a variety of sources such as research articles, and predicting future applications of this field based on the current applications.

2.1 - Fundamental Quantum Computing Vocabulary

This section of the paper will include fundamental quantum computing vocabulary, which you will need to be familiar with before reading about more advanced mathematics and rigorous algorithms.

1) Qubit

- a) In the classical world, computers operate on bits which take on the values of 1 and 0. However, quantum computers operate on quantum bits (known as qubits) which harness quantum physics properties such as quantum superposition and quantum entanglement to make processing power, memory, and time complexity of algorithms much faster.

2) Quantum state

- a) A quantum state measures the possibilities of a qubit's state. On classical computers, the state of qubits have to be either a 1 or 0; but, for quantum computers, the qubits take a more fluid identity, where there is a probability associated for the possible states it could be in. In [18], Ghose gives a very comprehensive overview of the most important quantum physics concept that one needs to know before progressing to higher level material.

3) Bloch sphere

- a) A Bloch sphere is a 3D geometrical space that is used to visualize the quantum state and its position with respect to the axes.

4) Quantum superposition

- a) Quantum superposition is one of the most popular quantum physics concepts. Qubits that are in quantum superposition have the ability to exist in multiple states simultaneously. This enables algorithms to run exponentially faster and opens up many new pathways.

5) Quantum entanglement

- a) Quantum entanglement, along with superposition, is also another widely known quantum physics concept. When two particles are quantum entangled, their quantum states depend on each other no matter how large the distance between these states are. Simply put, an entangled qubit's state can easily be determined if we know the other qubit's state because both of them can depend on one another.

The next sections of the review paper will immerse deeper into quantum circuits, quantum algorithms, and the advanced linear algebra math needed for this domain.

3. Gates

Logic gates are typically used for mechanical or electrical devices such as switches called transistors where electronic circuits can be combined with programming to perform preferred operations. In classical terms,

logic gates are basic devices of any digital circuit. They operate on bits and require an input and an output to function. To understand quantum gates, it is helpful to be familiar with the classical gates. The common ones in classical computing are the AND, OR, XOR, NOT, and NAND gates.

A classical computer evaluated a function and gives outputs based on the inputs. The amount of inputs might differ, from 1, 2 or 3, but today's logic gates are more familiar with a 2-input system with 1 output.

3.1 - AND Gate

The AND gate performs a boolean function with inputs false and true as "0" and "1," respectively. According to the truth table below, the output will be true when both inputs are also true. Otherwise, it will remain false. In other words, only an input of 1s will give an output of 1, as shown in the table [21].

Two Input AND gate		
A	B	$Y = A \cdot B$
0	0	0
0	1	0
1	0	0
1	1	1

Figure 1 - AND Gate

3.2 - OR Gate

The OR gate operates in a similar intuitive way. This time, if at least one true is inputted, the output will also be true. [21]

Two Input OR gate		
A	B	$Y = A + B$
0	0	0
0	1	1
1	0	1
1	1	1

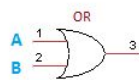


Figure 2 - OR Gate

3.3 - XOR Gate

The XOR gate, also known as the exclusive OR gate outputs 1 when the number of 1s inputted is odd [21].

Two Input XOR gate		
A	B	$Y = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

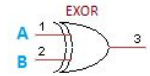


Figure 3 - Exclusive OR Gate

3.4 - NOT Gate

The NOT gate is also known as an inverter gate because it performs logical negation on its input. Simply, if the input is true, the output is false and vice versa.

3.5 - NAND Gate

The NAND gate acts like an AND gate followed by a NOT gate. The outputs will be 1 if at least one 0 is inputted [21].

Two Input NAND gate		
A	B	$Y = \overline{A \cdot B}$
0	0	1
0	1	1
1	0	1
1	1	0

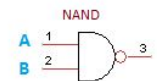


Figure 4 - NAND Gate

Now that the basic logic gates are summarized, quantum circuits provide a similar model of computation. Like logic gates operate on bits, quantum gates operate on qubits. This allows information to be conserved, a phenomenon known as unitarity, where there is no loss of info and the operation is reversible. An important concept relating to qubits is superposition, the linear combination of spins- $|0\rangle$ is an up spin, $|1\rangle$ is a

down spin, where α is the amplitude and $|\psi\rangle$ is a form for a matrix. In these cases, there is always the same number of inputs as outputs. The single qubits gates are the X gate and the Hadamard gate.

3.6 - X Gate

The X gate flips the superposition of a qubit. So the $|0\rangle$ state flips to the $|1\rangle$ state and the $|1\rangle$ state flips to the $|0\rangle$ state. To show this mathematically, we use matrices and matrix multiplication. The X gate is represented by [22]

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The function of the X gate operation uses the matrix multiplication shown below, converting $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$.

$$\begin{array}{lcl} |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \xrightarrow{\quad} & X \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \cdot 1 + 1 \cdot 0 \\ 1 \cdot 1 + 0 \cdot 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \\ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \xrightarrow{\quad} & X \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \cdot 0 + 1 \cdot 1 \\ 1 \cdot 0 + 0 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \end{array}$$

Figure 5 - X Gate Matrix Multiplication

3.7 - Hadamard Gate

The Hadamard gate converts a qubit to a uniform superposed state, rotating $|0\rangle$ and $|1\rangle$ to $|+\rangle$ and $|-\rangle$ respectively. In other words, $|0\rangle$ becomes $|0\rangle+|1\rangle$ while $|1\rangle$ becomes $|0\rangle-|1\rangle$.

Similar to the matrix multiplication computed for the X gate, the Hadamard gate is represented as follows [23]:

$$HH^\dagger = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^\dagger = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Figure 6 - H Gate Matrix

3.8 - CNOT Gate

The CNOT gate (also known as C-X or controlled-not) is a two qubit operation gate. The qubit is usually called the control, while the other is the target. It operated under the following conditions:

When the control is $|0\rangle$, the target qubit is left unchanged.

When the control is $|1\rangle$, an X gate is performed on the target qubit.

The CNOT matrix is represented as [24]:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The matrix multiplication is represented as:

$$Q' = CNOT * Q = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_4 \\ \alpha_3 \end{bmatrix}$$

Figure 7 - CNOT Matrix

3.9 - CCNOT Gate

The Controlled CNOT gate, also known as the Toffoli, has two control qubits and one target.

When both control qubits are in state $|1\rangle$, an X gate is applied to the target qubit.

The matrix is represented by [25]

$$TOFFOLI = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Figure 8 - Figure CCNOT Gate Matrix

Although there are many more quantum gates, the X, Hadamard, CX and CCX are most common ones and are most vital to understanding the calculator functions and various things we can further explore in the quantum mechanics world. The significance of quantum gates will be made more clear when discussing the various applications of quantum computing and the algorithms entailed. In general, these gates leverage the ideas of superposition and entanglement, an essential aspect of the field.

4. Addition

A classical computer computes basic mathematical operations at a hardware level using a digital electronic circuit, the arithmetic logic unit (ALU), allowing the buildup of logic gates and more complicated operations. When a math problem is typed on a keyboard, electrical signals are sent to the ALU, the operations are performed then come back in the form of electrical signals which turn into pixels on the screen. Quantum processors can take in information by themselves or with a classical processor, without the use of electrical signals. The IBM Qiskit platform processes information by making calls to a quantum processor even when classical functions are inputted.

To show how addition works on a quantum level, it is important to understand addition in a classical sense. When learning addition, kids are taught to add the numbers in the units column first, carry to the next leftmost column, and continue. Computers work the same way except using only binary digits, 1 and 0, as possibilities. The two operations included in this system is carrying and summing.

Quantum computers use the same system, just with qubits instead of classical bits, and stored values instead of directly outputted. The first step to writing a code of digital circuits that would allow for addition is to convert each step into gates.

The first computation is the carry gate, which requires 3 bits. The first step would be to compare qubits a and c. If they're both in state 1, flip the next bit. If qubit a is in state 1, flip qubit b. If qubits b and c are in state 1, flip the output bit. Since no one gate can represent this, we use a combination of CCX and CX gates as illustrated below. The purple gate on the ends is the CCX gate, and the blue gate in the middle is the CX gate. The image below was created using IBM Q Experience.

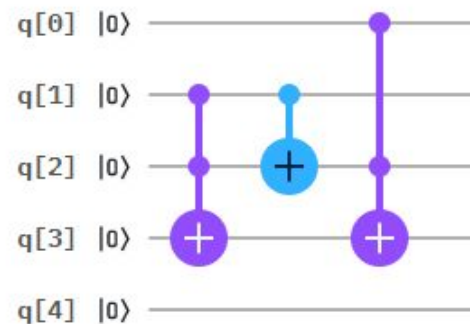


Figure 10 - Addition Carry Operation Circuit

Next, we compute the sum operation, also requiring three input gates, two for adding, and one for the carry gate. If the input carry qubit is in state 1, flip the qubit from the b register. Flip it again if the one from a is also in state 1. These steps can be achieved using CX gates, as illustrated below by IBM Q experience.

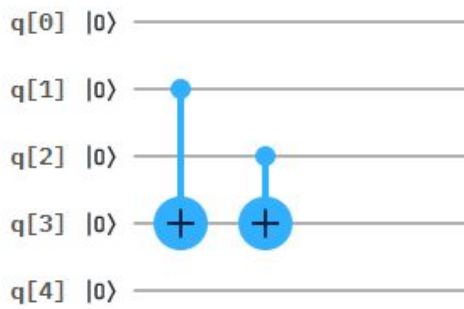


Figure 11 - Addition Sum Operation Circuit

To implement a complete quantum adder, two numbers need to be initiated as inputs. Next the registers need to be combined to create a quantum circuit. Since values cannot directly be assigned to quantum registers, another quantum register needs to be created. After implementing the summing and carrying gate operations, the visualization, along with results, can be seen below, also created using the IBM Q Experience platform.

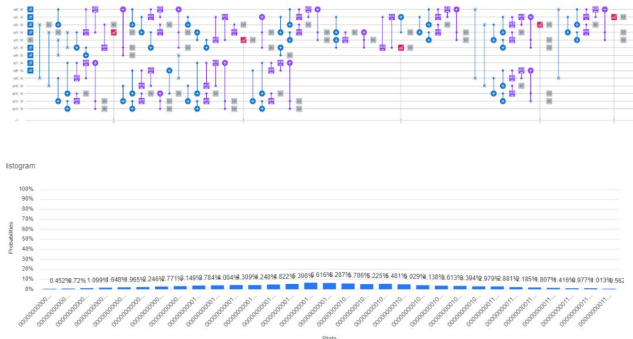


Figure 12 - Addition Circuit

5. Subtraction

Quantum circuit for subtraction operation is very similar to quantum addition. The only difference is that we need a negative sign before the second number.

When we rotate the qubit, we place a negative sign in front of the angle.

The subtraction operation uses the same circuit as the addition operation.

6. Multiplication

Before delving into how a quantum computer performs multiplication, it's necessary to first understand how a classical computer multiplies two numbers.

How a classical computer multiplies two numbers -

To demonstrate this process more effectively, let's take the following example.

Let $a = 250$ and $b = 24$. Our goal is to get the product of a and b .

$$\begin{array}{r}
 250 \\
 \times 24 \\
 \hline
 1000 \\
 + 500 \\
 \hline
 1500
 \end{array}$$

In this scenario, the 250 is called a multiplicand and 24 is the multiplier [20].

According to [20],

- 1) The computer first multiplies the multiplicand (1000) with 4, the rightmost digit of the multiplier.
- 2) It repeats step 1 but does it for the other digit of the multiplier. For both of these steps, it stores each of these products as "partial products."
- 3) Then, to sum the partial product, it first shifts the second product to

ensure both numbers are lined up correctly.

- 4) Then, these partial products are added together to get the final answer of the product.

Because multiplication is simply addition repeated several times, we need to use the addition algorithm. We can either opt for a faster method using quantum fourier transformation (QFT) or the simpler method which uses CX and CCX gates. We are going to continue with the approach of using QFT to add two numbers since it's much faster.

The QFT algorithm decomposes a given input into its constituents. For instance, if a program is fed a very complex wave, it can be broken down into a set of simpler waves, which is what QFT achieves. This decomposition is achieved through several rotations, which can be performed by the Hadamard gates and controlled R gates.

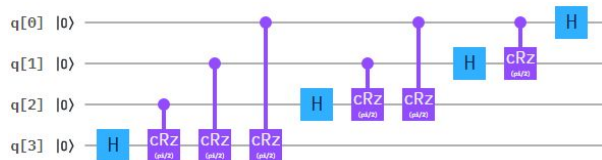


Figure 13 - Multiplication Circuit

Credits - Circuit built from IBM Q Experience

We need quantum fourier transformation adder to understand the multiplication operation algorithm as described below.

Multiplication Operation Algorithm (according to [20]) -

We are given a multiplicand and multiplier as input and want to obtain the product of them.

- 1) To accumulate the sums of the partial products, we need a new quantum register that will store this value. Let us denote it as R.
- 2) We will repeat this step till the multiplier reaches 0 value.
 - a) Add the multiplier to the multiplicand. Then, add this value to R.
 - b) After every sum operation, decrease the multiplier using the subtraction algorithm discussed in section 5 of this paper.
- 3) At the end, we can obtain the output from register R.

7. Division

Although there have been thorough studies in the quantum implementation of division, no one has addressed an explicit quantum circuit of division. Instead, we will discuss the theoretical background such as a quantum shift register, quantum adder and subtractor and quantum fourier transform which builds off theorems like Grover's algorithm and Shor's algorithm.

A quantum shift register is useful when shifting a number to a different register. The classical shift operation loses qubits when the register is shifted, making the operation irreversible. Instead, the quantum operation uses ancilla qubits to store entangled states, enabling a reversible option. Below is an implementation of a quantum circuit for the left shift operation [26].

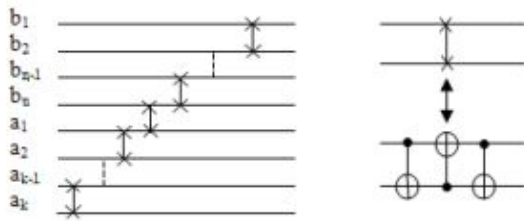


Figure 14 - Quantum Shift Register

The quantum fourier transform is a linear transformation of finite sequences. This is especially helpful for Shor's algorithm, the discrete logarithm and the quantum phase estimation algorithm. It is essentially the decomposition into a product of matrices. The circuit is composed of conditional rotation and Hadamard gates. One example is shown below [27].

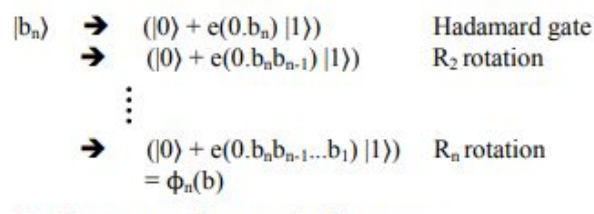


Figure 15 - Quantum Fourier Transform

Implementing division with the quantum addition and subtraction methods makes the division circuit more efficient as it eliminates the use of extra qubits and is similar to the quantum fourier transform.

The restoring division algorithm is the most straightforward implementation of quantum division. The basis is outlined as [14]:

Step-1: The registers are initialized with values (Q = Dividend, M = Divisor, $A = 0$, n = number of bits in dividend)

Step-2: The content of register A and Q is shifted right

Step-3: Then content of register M is subtracted from A and the result is stored in A

Step-4: The most significant bit of the A is checked if it is 0. If the least significant bit of Q is set to 1, it is then set to 0. The value of register A is restored.

Step-5: The value of counter n is decremented

Step-6: If the value of n becomes 0 we get of the loop otherwise we repeat from step 2

Step-7: Finally, the register Q contain the quotient and A contain remainder.

From these steps, the inclusion of the quantum register, the quantum fourier transform, and the addition and subtraction operations makes sense as it provides the theoretical background of a possible quantum division circuit.

8. Applications (Shor's Algorithm, etc.)

As discussed in section one of this paper, quantum computing has great potential in various areas.

8.1 - Cryptography

One particular application lies in the quantum cryptography realm - Shor's Algorithm. The classical computing algorithm for cryptography is the asymmetric RSA algorithm (Rivest-Shamir-Adleman), which encrypts and decrypts messages in a secure fashion. An asymmetric algorithm in cryptography uses two keys, where the public one is accessible to anyone who wants to encrypt their message and the private one cannot be shared with anyone else when decrypting the message. This modern cryptography algorithm is centered around

the idea of multiplying two very large prime numbers, n and p . When encrypting, these two numbers are multiplied to form one huge number np . When it comes to encrypting this message, this number np is broken down to its original prime factors n and p . However, one of the main problems of this classical computing problem is the computer can only take so large numbers and compute its factors in an efficient time complexity. Currently, one of the most efficient solutions we have in the classical realm is the number field sieve, as discussed in [2]. However, this algorithm still has its limitations when computing the factors of extremely large numbers - its time complexity is very slow on classical computer. Thus, Shor's algorithm was one very good quantum solution to this issue.

Back in 1996, the mastermind of this cryptography algorithm, Peter Shor developed a quantum solution presented in his paper. In [3], he utilizes quantum gates to perform unitary transformations on qubits along with Quantum Fourier transformation and various principles of quantum physics to construct his efficient algorithm.

Something very important to note about Shor's algorithm is that it can be run on both a classical and quantum computer. While it does run on both types of computers, it runs significantly faster on a quantum computer. This algorithm opens up integer factorization of immense numbers since we can afford to compute integer factorization in efficient time complexity by deploying a quantum circuit on a quantum computer or simulator, as provided by IBM Quantum Experience.

8.2 - Shor's Quantum Algorithm in Pseudocode

1. Pick an arbitrary number N . This will be the integer that we are trying to find factors of.
2. Let us define our random guess to be g . g has the possibility of being a factor. g We do not need g to be a factor.
3. Transform g into a better guess which will probably share at least one factor of N by following the following substeps.
 - a. Let there exist two arbitrary numbers p and n . This better guess will be equivalent to $g^{(p/2)} \pm 1$. This is because of a proof [7] which demonstrates that $g^p = (m * N) + 1$. Further simplifying and factoring this equation will lead us to obtain the better guess to be $g^{(p/2)} \pm 1$. Once we obtain the two better guesses ($g^{(p/2)} + 1$ and $g^{(p/2)} - 1$), we can apply the Euclidean algorithm on them to get the factors of our original number N .

The central reason why Shor's cryptography algorithm will run so efficiently on a quantum computer because a quantum computer harnesses quantum physics; more specifically, it utilizes superposition to calculate all of the answers simultaneously. Furthermore, the notion of wave constructive and destructive interference are integral to understanding the quantum physics - all of the wrong answers will destructively interfere and the correct answer will not have a destructive interference so it will be very quick and easy to identify the solution to this cryptography problem.

8.3 - Teleportation

Besides quantum cryptography, another popular quantum application is teleportation. While we are not close to teleporting humans, we have made great progress in teleporting particles. While some may know teleportation as relocating a body to another place or disassembling models and reassembling them, quantum teleportation refers to the building of an entirely new body with the same information. It has been known since the 1990s that quantum teleportation was possible but it wasn't until recently that [9] Chinese scientists have made an unprecedented discovery - they have teleported packets of information to space. Specifically, they transmitted the quantum state of a photon on Earth to a satellite on Earth's orbit in space about 1400 kilometers away. To date, this is the farthest distance we have achieved for teleportation. This type of transmission is what is known as quantum teleportation. Other than photons, electrons and even calcium atoms have been teleported.

This is possible due to the mechanism of quantum entanglement, where two or more particles hold mutually exclusive states. The states of an object aren't independent of each other. For example, atoms can be entangled if the outer orbital of one moves to the left, while the orbital of another moves to the right. They are always contained as opposites, so if one state is known, the other is as well. Entanglement can be maintained over arbitrarily long distances, giving rise to the idea of teleportation. When an entangled pair is transmitted, one imprints the state of the object, while the other ends up as the

opposite, or negative, of that imprinted state. This results in the teleportation of an object.

A particular implication which is especially remarkable is in long distance communication: eavesdroppers will not be able to eavesdrop on this type of system without alerting the other side. With quantum teleportation, the phenomenon of entanglement makes it easy to decipher communication. Currently, if a message is to be sent, it cannot be done without accompanied classical information, defeating the purpose of communication on a quantum level.

In the future, however, qutrit experiments are to take over. Some scientists are attempting to teleport more complex states, while others are trying to increase the number of particles involved. While trying to teleport more complicated states of atoms, qubits (binary states) are still being used. This introduces the idea of a qutrit, a superposition embodying a state of 0, 1 or 2. Experiments are currently being done on entangled qutrits to try to create this type of quantum system to successfully encode information for eventual communication. Despite the current efforts, the main goal of quantum teleportation is to teleport a higher proportion of quantum information, leading to better quantum communication networks.

8.4 - Quantum AI/ML

Machine learning, a subset of artificial Intelligence, is a field of computer science where robots acquire human intelligence through training and various statistical models. There are mainly three types of artificial intelligence - Unsupervised, Supervised, and Reinforcement learning.

Many different AI algorithms (lying mainly in the classification, regression, and clustering domains) are used to solve computational problems and train the machine

One widespread application of Quantum Computing is Quantum Artificial Intelligence and Quantum Machine Learning.

Artificial Intelligence and Machine Learning have long been talked about because of the broad impact they have on our real world. However soon, there will be a lot more emphasis on Quantum AI and Quantum ML once quantum algorithms become more feasible in the real world because of the tremendous efficiency power they have.

On traditional computers with bits, one of the most popular AI algorithms that is run is the neural network. Neural networks are algorithms that involve training the machine by identifying patterns using some objective function, weights, and input data. Furthermore, the algorithm involves many hidden layers, where the computation and statistical models are run. Once the machine is trained in the hidden layers and is able to identify patterns, it can make powerful predictions. From advancing the medical industry to predicting powerful financial changes, neural networks have many broad and deep affects.

To make the leap from the classical to the quantum realm for machine learning / deep learning, there are many steps taken using quantum gates [29]:

1) Quantum- In the first layer of the network, the input vector is encoded using the quantum states

- a) Classical- A unit vector is passed on to the hidden nodes, where a functions (Ex-sigmoid) will be used for the calculations.

2) Quantum- Using quantum gates, many unary transformations are performed on the qubits.

- a) Classical- This step is analogous to the classical algorithm, where a weighted sum is computed from the input vectors.

3) Quantum- The ancilla qubit stores the output, which is equivalent to the entangled state of the qubit.

- a) Classical- Once the hidden neurons perform the computations, the neural network returns an answer through the output neurons.

Overall, there are many prevalent advantages of a quantum neural network over a classical neural network- the memory capacity is exponential, there is much faster learning, it's a more stable system, and the network has a faster processing speed.

In the quantum world, using a Hopfield network, Xanadu has developed a Quantum Neural Network (QNN), which achieves the same goal as a classical neural net. [11]













states	$ \uparrow\uparrow\rangle$	$ \uparrow\downarrow\rangle$	$ \downarrow\uparrow\rangle$	$ \downarrow\downarrow\rangle$	coherent superposition
					$\frac{1}{2}(\uparrow\uparrow\rangle - \uparrow\downarrow\rangle - \downarrow\uparrow\rangle - \downarrow\downarrow\rangle)$
configurations					$\frac{1}{2}(- \uparrow\uparrow\rangle + \uparrow\downarrow\rangle + \downarrow\uparrow\rangle - \downarrow\downarrow\rangle)$
					$\frac{1}{2}(\uparrow\uparrow\rangle - \uparrow\downarrow\rangle + \downarrow\uparrow\rangle + \downarrow\downarrow\rangle)$
					$ \uparrow\rangle = \text{"up"} \quad \downarrow\rangle = \text{"down"}$

Figure 16 - Quantum Neural Network

Steps that Xanadu used to develop a QNN [15] -

- 1) Using a quantum physics property called quantum superposition (refer to section one (Introduction) to see the

definition), each neuron can exist in multiple states simultaneously.

- 2) Choose a Hopfield network for the neural network, which is a recurrent neural net and has several weighted edges between the nodes of the graph. Xanadu chose the Hopfield network, in particular, because it's a great mechanism to store different patterns using the different connections between the nodes.
- 3) Instead of repetitively updating the weights attached the edges (as the regular machine learning model does), the algorithm Xanadu used (HHL algorithm [16]) inverts a matrix
 - a) To utilize this matrix inversion algorithm, Xanadu performed a Hamiltonian simulation of their quantum system. [11]

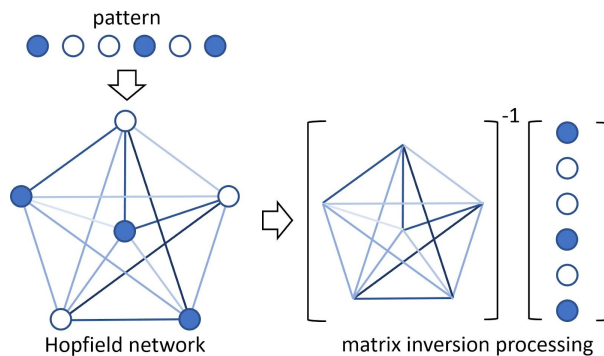


Figure 17 - Quantum Neural Network 2

Through their exponentially fast quantum neural network, Xanadu was able to show that their results on real world applicable problems such as in the biology domain turn out to run dramatically faster using a quantum computer.

Another popular machine learning algorithm is clustering. Specifically, tools like k-means clustering are very popular. In this algorithm, the points are divided into k

clusters by using the distance (oftentimes the euclidean distance) to measure the distance between centroids. The quantum version of the algorithm achieves the same result by calculating the distance from each state to every other state. It is critical to note that these quantum states are many times in quantum superposition. After representing these quantum states in a vector form, linear algebra mathematics is applied to compute the distances. There are two main steps - converting the coordinates in the classical system to a system which can be used by a quantum computer [17]. After this conversion, [17] computes and compares the distances between these quantum states which helps with building these clusters.

Decision tree algorithms are widely used in our daily lives when we make decisions based on a set of circumstances given. Through a concept called entropy, which measures the amount of disorder present in a system, ML scientists have constructed a model that decreases in entropy as you go further down the tree. In other words, as we progress to the bottom nodes of this tree, we approach more defined outcomes, which is why the overall Shannon entropy tends to decrease. Currently, there is not one exact quantum algorithm which maps this ML algorithm to quantum processors. However, we do know that we need to harness a quantum physics property called Von Neumann Entropy, which is parallel to the Shannon entropy used for the classical decision trees.

The machine learning k nearest neighbors algorithm has been used in many types of problems where pattern recognition is essential. Given an input consisting of a set of points, the algorithm uses a distance

parameter (oftentimes the simple Euclidean distance) to sort the distances between one point to the others. It repeats this process for all the points and after this sorting is able to obtain the k closest ones [29] to the queried point. To achieve this same objective, the quantum algorithm uses the Quantum Swap Test, which helps us determine what the overlap is between two given quantum states and how much they differ. This similarity measure is obtained through the Hadamard logic gate, which puts a qubit into superposition of many states. After this test, the distance is easily determined and the nearest neighbors are then outputted.

Another powerful quantum machine learning algorithm is the Quantum Generative Adversarial Network (QGAN). In the classical unsupervised machine learning domain, GAN uses two neural networks (the discriminator and the generator) which compete with each other until they reach an equilibrium point. This concept is a very popular game theory computer science concept called the “Nash Equilibrium.” The purpose of this competition between the neural networks is to train the model to identify which datasets are part of the true data set and which aren’t. Instead of two neural nets, the QGAN [28] has two quantum circuits (generator and discriminator circuits). Then, noise and the state is inputted into the generator state and the generator circuit feeds the discriminator circuit various types of fake data. To update the parameters of the algorithm, the quantum circuit computes a gradient. While in the classical world a gradient descent is used to minimize the error function for the GAN so we get values which are closer to the actual number, in the quantum world, the quantum circuits compute this gradient for quantum optimization of the algorithm.

There are many parallels between the classical and quantum algorithms in artificial intelligence/ machine learning/ deep learning. In many of these algorithms, quantum physics concepts such as superposition and entanglement are used when converting the state to a quantum state through the various quantum gates. This transitioning step is highly critical to create robust quantum AI/ML algorithms!

8.5 - Financial Modeling

Involving quantum computing in business can revolutionize financial solutions to problems such as dynamic portfolio optimization, clustering, scenario analysis, and option pricing. The connection between finance and quantum computing stems from the idea of uncertainty, whether this is predicting profit or competing with others, financial practitioners deal with the impossibility of knowing these predictions.

Optimization is the idea of maximizing returns given certain risks. Classical computers often have difficulty solving these complicated equations, making a quantum solution ideal. This specific process is called quantum annealing. This involved turning physical problems into models using energy states and mathematical expressions. For instance, trade is commonly influenced by optimization because of market risks and slow trading impacts. Loans are given with uncertainty when predictions of credit score and financial history are taken into account.

Within the field of data classification, quantum machine learning proves its importance. This is done by expressing customers as vectors and characteristics as

coordinates. Implementing experiments and algorithms can be done more efficiently on quantum computers.

Another financial application involves a concept known as quantum amplitude estimation. This works by sampling scientific applications and stimulating the effects of these distributions. However, this usually involved a significant amount of error. Quantum amplitude estimation samples a probabilistic distribution faster than done on classical computers. Specifically, this can be used to calculate the growing number of derivative products without computational costs and lengthy execution times. This algorithm can also be used to quantify risks through a distribution portfolio to determine the 'value at risk' function exponentially faster than classical computers.

9. Conclusion & Next Steps

This paper gave a summary which covered all of the breakthroughs and research that has been conducted in the field. Along with showing the progress we have made when making the leap from the classical to the quantum realm, this paper compares the different quantum algorithms for various domains (the purpose of each algorithm and its practical uses in the real world).

Quantum computing is a very revolutionary, powerful field that is being leveraged in many real world applications today. However, it has the power to become even more powerful in the near future. In particular, new quantum algorithms will be developed for current machine learning algorithms such as the ML decision tree. Developing new quantum ML algorithms will enable us to feed more massive datasets and get more accurate conclusions. Moreover,

quantum algorithms will solve currently open and seemingly impossible problems on traditional computers.

Another potential application of quantum computing is weather forecasting. Today, even though we have machine learning models, there is still much uncertainty because of the complexity and the multitude of variables [19]. Quantum computers will not only be able to drastically reduce this error but also forecast accurately for much longer time periods.

A very exciting use of quantum computing in our future is space exploration. Through quantum computing, the process of discovering new planets will accelerate greatly since churning large cluttered datasets will be much smoother and faster [19].

Along with discovering new drugs which can greatly help the medical/ biology/ chemistry industry, this field has the potential to create an environment with perfectly secure communication and data (through algorithms like Shor's algorithm which will be used in cryptography domain), which is not possible today, even with the supercomputers we have.

Soon, we will be able to make the impossible possible through quantum computing!

10. References

- [1] A. Steane, "Quantum computing".
- [2] M. Case, "A Beginner's Guide To The General Number Field Sieve."
- [3] P. Shor, "Polynomial-Time Algorithms for Prime Factorization

and Discrete Logarithms on a Quantum Computer*," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*.

[4] W. Sangosanya , D. Belton, and R. Bigwood, "Basic Gates and Functions."

[5] "Quantum Computation," *Caltech Particle Theory*.

[6] M. Prasad, P. Bikkuri, N. Manaswini, "Operation of logic gates (AND, NAND, OR, NOR) with single circuit using BJT (Bipolar Junction Transistor)," *International Journal Of Advanced Research, Ideas and Innovations in Technology*, vol. 5, pp 1-3.

[7] Reich, H. [minutephysics] (2019, April 30). How Quantum Computers Break Encryption | Shor's Algorithm Explained[Video File].

[8] S. Anagolum, "Arithmetic on Quantum Computers: Multiplication," *Medium*, 08-Dec-2018.

[9] J. Emspak. "Chinese Scientists Just Set the Record for the Farthest Quantum Teleportation," *Space*, July 15, 2017.

[10] S Singh, P Ratnaparkhi, B Behera, P Panigrahi, "Demonstration of a Quantum Calculator on IBM Quantum Experience Platform and its Application for Conversion of a Decimal Number to its Binary Representation," Oct 04 2018.

[11] T. Bromley, "Making a Neural Network, Quantum," *Medium*, Feb 20, 2018

[13] S. Anagolum, "Arithmetic on Quantum Computers: Addition," *Medium*, Sep 8, 2018.

[14] S. Maurya, "Restoring Division Algorithm For Unsigned Integer," *GeeksforGeeks*.

[16] A. Harrow, A. Hassidim, S. Lloyd, "Quantum algorithm for solving linear systems of equations," vol. 15, no. 103, pp. 150502, 30 Sep 2009.

[17] S. Anagolum, "Quantum machine learning: distance estimation for k-means clustering" *Towards Data Science*.

[18] Ghose, S. [TED] (2019, February 1).A beginner's guide to quantum computing | Shohini Ghose [video file].

"[19] D Tal, "How Quantum computers will change the world: Future of Computers P7," *Quantum Run*.

[20] Sangosanya , Wale, et al. "Basic Gates and Functions." *Basic Gates and Functions*, <http://www.ee.surrey.ac.uk/Projects/CAL/digital-logic/gatesfunc/#notgate>.

[21]"Basic Logic Gates Truth Table." *Theory Circuit*, <http://www.theorycircuit.com/basic-logic-gates-truth-table/>.

[22] Kerr, John, "Quantum Computing #1: Single Qubit Gates," 16 October 2011.

[23] Truong, Quentin, "Introduction to Quantum Programming," 5 August.

[24] Liu, Wenjie, Xu, Yinsong, Zhang, Majojun, Chen, Junxiu, Yang, Ching-Yung, "A novel Quantum Visual Sharing Scheme," 2016.

[25] Kragler, Robert, "A Mathematica Package for simulation of quantum computation", Sep. 2009.

[26] Khosropour, Alireza , Aghababa, Hossein, Forouzandeh, Behjat, "Quantum Division Circuit Based on Restoring Division Algorithm," April 2011.

[27] J. Hui, "QC — Quantum Fourier Transform," *Medium*, Dec 13, 2018.

[28] Situ, Haozhen, He, Zhimen, Wang, Yuyi, Lvzhou, Shenggen, Zheng, "Quantum generative adversarial network for discrete data." Elsevier, Oct. 2019.

[29] Schuld, Maria, Sinayskiya, Ilya, Petruccionea, Francesco, "<https://arxiv.org/pdf/1409.3097.pdf>", September, 2014.