Quantum Computation and Quantum Algorithms

Monit Sharma
Indian Institute of Science Education And Research Mohali
(Dated: July 8, 2021)

Why do we need Quantum Computers? Because they can help us solve complex problems, but not necessarily NP-Hard [1] problems. There are two main paths for the research regarding Quantum Computers: one has to do with developing algorithms, and the other is the construction of such hardware that help us in running such algorithms. Quantum computing began in 1980 when physicist Paul Benioff proposed a quantum mechanical model of the Turing machine.[2] Richard Feynman, and Yuri Manin later suggested that a quantum computer had the potential to simulate things a classical computer could not feasibly do.[3][4] In 1994, Peter Shor developed a quantum algorithm for factoring integers with the potential to decrypt RSA-encrypted communications. Despite ongoing progress, many still believe that fault-tolerant[5] quantum computing is still a distant dream. In this paper Part I, we'll see the basics of Quantum Computing and Quantum Gates, Qubit Systems and their measurements and Quantum Entanglement. In the Part II, we'll see some Quantum Algorithms that use the above mentioned properties, namely the Quantum Key Distribution ,CHSH Game and Quantum Teleportaion.

I. INTRODUCTION

A. Quantum Computer

Quantum Computing is a computing paradigm that exploits quantum mechanical properties, such as superposition, entanglement, interference of matter in order to do calculations. It is not possible to commercially produce and maintain a Quantum Computer. The main reason is the property of Quantum Decoherence. Quantum Decoherence is the loss of coherence or balance of a Quantum Particle on its exposure to the environment. If thermal energy is continuously lost, then the Qubit spin slows down and results in inconsistent measurements. Notably, quantum computers are believed to quickly solve specific problems that no classical computer could solve in any feasible amount of time—a feat known as "quantum supremacy." Various organizations have made their quantum computer using different technologies in the hope of achieving Quantum Supremacy.The field of quantum mcomputing explores how to devise and implement quantum software that could enable learning that is faster than that of classical computers.

- Superconducting Loops , used by Google and IBM, They are fast, and are build on an existing semiconductor industry, but they must be kept cold because the collapse early.
- Trapped Ions , used by Icon-Q, They are very stable, and have highest achieved gate fidelities, but they are slow and need many Lasers to work.
- Silicon Quantum Dots, used by Intel, They are stable, and build on an existing semiconductor industry, but only a few are entangled and they also must be kept cold.
- Topological Qubits, used by Microsoft and Bell Labs ,They greatly reduce the errors , but their existence is not yet confirmed.
- Diamond Vacancies, used by Quantum Diamond Technologies, They can be operated at room temperature, but are very difficult to entangle.

Elements of a Quantum Circuit

Every computation has three elements: data, operations and result.

In a Quantum Circuit, the data is encoded in the Qubits, the operations are the Quantum Gates that we apply. which are Unitary transformations, and we get the result by measuring the Qubits.

B. One-Qubit System

A classical bit can take two different values (0 or 1). It is discrete. A Qubit can "take" infinitely many different values. It is continuous, Qubits live in a Hilbert Vector Space, with a basis of two elements that we denote $|0\rangle$ and $|1\rangle$. A generic qubit is in a Superposition when,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1$$

Measuring a Qubit is the only way to get concrete information from our Quantum Circuit. The result of the measurement is random and when we measure, we only obtain one bit of information. We cannot perform several independent measurements of $|\psi\rangle$ because we cannot copy the state (aka the No Cloning Theorem)[6]

1. Quantum Gates

Quantum Mechanics tells us that the evolution of an isolated state is given by the Schrodinger equation

$$H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$$

In case of Quantum Circuits, this implies that the operations that can be carried out are given by unitary matrices. That is, Matrices U of complex numbers verifying

$$UU^\dagger = U^\dagger U = I$$

where $U^\dagger$ is the conjugate transpose of U.

Each such matrix is a possible quantum gate in a Quantum Circuit.

Consequently, all the operations also have an inverse, and we term this as"Reversible Computing". Every Quantum gate has the same number of inputs and outputs. Not to be confused with the classical gates. However, we cannot directly implement some classical gates such as OR, AND, NAND, XOR. What we can do is simulate any classical computation with a small overhead.

2. One-Qubit Gates

When we have just one qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we usually represent it as a column vector

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

Then, a one-qubit gate can be identified with a matrix

$$U = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

that satisfies..

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\bar{a} & \bar{c}\\ \bar{b} & \bar{d}\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

where $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ are the conjugates of Complex numbers a, b, c, d.

We can see the action of a One-Qubit Gate by simple matrix multiplication. A state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is transformed to

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}a\alpha + b\beta\\ c\alpha + d\beta\end{pmatrix}$$

hence, the state $|\psi\rangle$ is transformed into the state $|\psi\rangle = (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle$

Since the U is unitary , it also holds(the probabilistic sum)

$$|(a\alpha + b\beta)|^2 + |(c\alpha + d\beta)|^2 = 1$$

C. Two-Qubit Systems

For a two-qubit system each qubit can be in state $|0\rangle$ or in state $|1\rangle$. So for two qubits we have four possibilities:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

that we also denote by:

$$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$$

or

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

and there are superpositions in this case, so a generic state is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where α_{xy} are complex numbers such that

$$\sum_{x,y=0}^{1} |\alpha_{xy}|^2 = 1$$

Measuring a two-qubit system is similar to that of a one-qubit system. Suppose we have a state

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

If we measure both qubits, we will obtain:

- 00 with probability $|\alpha_{00}|^2$ and the new state will be $|00\rangle$
- 01 with probability $|\alpha_{01}|^2$ and the new state will be $|01\rangle$
- 10 with probability $|\alpha_{10}|^2$ and the new state will be $|10\rangle$
- 11 with probability $|\alpha_{11}|^2$ and the new state will be $|11\rangle$

It is analogous to to what we had with one qubit, but now with four possibilities.

Two-qubit state and vector representation

A general two-qubit quantum state is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

We can represent with the column vector.

$$\begin{pmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{pmatrix}$$

We can compute the inner product by noticing that

$$\langle 00|00\rangle = \langle 01|01\rangle = \langle 10|10\rangle = \langle 11|11\rangle = 1$$

$$\langle 00|01\rangle = \langle 00|10\rangle = \langle 00|11\rangle = ... = \langle 11|00\rangle = 0$$

A two-qubit quantum gate is a unitary matrix U of size $4 * 4$.

The simplest way of obtaining a two qubit gate is by having a pair of one-qubit gates A and B acting on each of the qubits.

In this case, the matrix for the two-qubit gate is the tensor product $A \otimes B$

It holds that

$$(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A|\psi_1\rangle) \otimes (B|\psi_2\rangle)$$

Either A or B may be the identity.

D. Multiple Qubit Systems

For a n-qubit systemm, When we have n qubits, each of them can be in state $|0\rangle$ and $|1\rangle$ Thus, for the n-qubit state we have 2^n possibilities:

$$|000.....0\rangle, |000.....1\rangle, ..., |11.....1\rangle$$

or simply

$$|0\rangle, |1\rangle, ..., |2^n - 1\rangle$$

A generic state of the system will be

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + ... + \alpha_{2^n-1}|2^n - 1\rangle$$

Measuring a n-qubit state

If we measure all its qubit, we obtain:

- 0 with the probability $|\alpha_0|^2$ and the new state will be $|00.....0\rangle$
- 1 with the probability $|\alpha_1|^2$ and the new state will be $|00.....1\rangle$
- .....
- $2^n - 1$ with probability $|\alpha_{2^n-1}|^2$ and the new state will be $|11.....1\rangle$

Measuring one qubit in a n-qubit state

We have

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + ... + \alpha_{2^n-1}|2^n - 1\rangle$$

If we measure the j-th qubit We will get 0 with probability

$$\sum_{i \in I_0} |\alpha_i|^2$$

where I_0 is the set of numbers whose j-th bit is 0.
In that case , the new state $|\psi\rangle$ will be

$$\frac{\sum_{i \in I_0} \alpha_i |i\rangle}{\sqrt{\sum_{i \in I_0} |\alpha_i|^2}}$$

E. Quantum Gates

1. X-Gate

The X gate is defined by the unitary matrix

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

It's action is denoted in the quantum circuit notation is denoted by

$$|0\rangle - - - [X] - - - |1\rangle$$

$$|1\rangle - - - [X] - - - |0\rangle$$

Hence it acts like a classical NOT gate.
On a general qubit its action is

$$\alpha|0\rangle + \beta|1\rangle - -[X] - -\beta|0\rangle + \alpha|1\rangle$$

2. Z-Gate

The Z gate is defined by the unitary matrix

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

It's action is

$$|0\rangle - - - [Z] - - - |0\rangle$$

$$|1\rangle - - - [Z] - - - (-|1\rangle)$$

3. H-Gate

The H or the Hadamard gate is defined by the unitary matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

Its action is

$$|0\rangle - - - [H] - - - \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle - - - [H] - - - \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

and the output states are generally denoted by $|+\rangle$ and $|-\rangle$

The Gates X, Y, Z are also called the Pauli gates. An alternative notation is $\sigma_x, \sigma_y, \sigma_z$.

4. CNOT Gate

The CNOT gate (or the controlled-NOT or cX) is given by the unitary matrix

$$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

If the first qubit is $|0\rangle$, nothing changes. If it is $|1\rangle$, we flip the second bit (and the first remains the same). That is

$$|00\rangle \to |00\rangle$$

$$|01\rangle \to |01\rangle$$

$$|10\rangle \to |11\rangle$$

$$|11\rangle \to |10\rangle$$

This is an extremely important gate for it allows us to create entanglement and entangled states, it helps in copying classical information and it can also construct other controlled gates.

5. Toffoli Gate

The Toffoli gate (or CCNOT) is a 3-qubit gate. Thus it can be represented as 8×8 matrix.

Its action on elements $x, y, z \in \{0, 1\}$ is : 1

The Toffoli gate is universal for classical logic, and thus any classical circuit can be simulated with a quantum circuit. However, the Toffoli gate, on its own, is not universal for quantum computing.

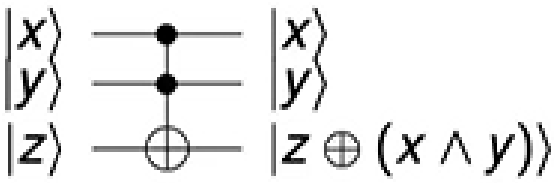

FIG. 1. Toffoli Gate

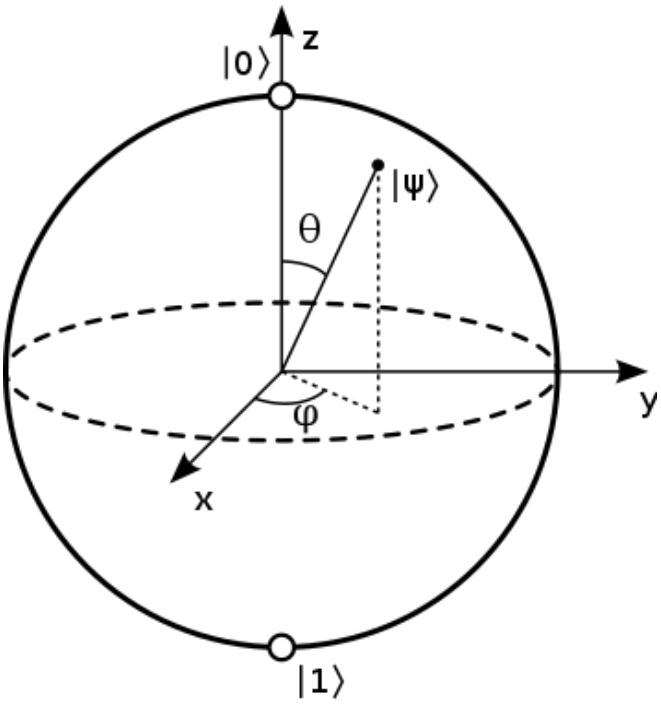

FIG. 2. A Bloch Sphere (Source:Wikipedia)

F. The Bloch Sphere

A common way of representing the state of a qubit is by the means of the point in the surface called as the Bloch Sphere.

If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, we can find angles γ, δ, θ such that

$$\alpha = e^{i\gamma} cos\frac{\theta}{2} \beta = e^{i\delta} sin\frac{\theta}{2}$$

Since the overall phase is irrelevant, we can rewrite

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi} sin\frac{\theta}{2}|1\rangle$$

with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$.

From $|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi} sin\frac{\theta}{2}|1\rangle$, we can obtain spherical coordinates for a point in $\mathbf{R}^3$

$(sin\theta cos\phi, sin\theta sin\phi, cos\theta)$

1. Rotation Gates

We can also define the rotation gates, with the help of phase angle and better visualization in the Bloch Sphere.

$$R_X(\theta) = e^{-i\frac{\theta}{2}X} = cos\frac{\theta}{2}I - isin\frac{\theta}{2}X$$

$$R_Y(\theta) = e^{-i\frac{\theta}{2}Y} = cos\frac{\theta}{2}I - isin\frac{\theta}{2}Y$$

$$R_Z(\theta) = e^{-i\frac{\theta}{2}Z} = cos\frac{\theta}{2}I - isin\frac{\theta}{2}Z$$

The inner product of two states $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ is given by

$$\langle\psi_1|\psi_2\rangle = (\bar{\alpha_1}\bar{\beta_1})\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \bar{\alpha_1}\alpha_2 + \bar{\beta_1}\beta_2$$

Notice that $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$

G. The No-Cloning Theorem

The no-cloning theorem states that it is impossible to create a copy of an arbitrary quantum state. Consider a quantum computer with two registers: the data register which is in state $|\psi\rangle$, and the target register which is in a particular state $|t\rangle$. Then, the no-cloning theorem is equivalent to saying that for every state $|\psi\rangle$, there is no unitary quantum circuit U that can transform the state to:

$$|\psi\rangle \otimes |t\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$$

There is no quantum gate that makes copies of an arbitrary qubit. The proof is easy: Suppose we have a gate U such that

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

Then $U|00\rangle = |00\rangle$ and $U|10\rangle = |11\rangle$ and by linearity

$$U(\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)) = \frac{1}{\sqrt{2}}(U|00\rangle+U|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

But

$$\frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle$$

so we should have

$$U(\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle + |1\rangle}{\sqrt{2}} \neq \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

H. Quantum Entanglement

We say that a state $|\psi\rangle$ is a product state if it can be written in the form

$$|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$$

where $|\psi_1\rangle$ and $|\psi_2\rangle$ are two states.

An entangled state is a state that is not a product state. Example of Entangled states (Bell States):

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

II. QUANTUM ALGORITHMS

In quantum computing, a quantum algorithm is an algorithm that runs on a realistic model of quantum computing. A classical (or non-quantum) system is a finite sequence of instructions or a step-by-step procedure for solving a problem, where each step or instruction can be performed on a classical computer. A quantum algorithm is a step-by-step process, where each step can be done on a quantum computer. Although all classical algorithms can be implemented on a quantum computer, the term quantum algorithm is often used for those algorithms that seem to be of quantum nature or have few of the essential features of quantum computing, such as quantum superposition or quantum entanglement.

A. Quantum Key Distribution and the BB84 Protocol

We will look at a practical application for quantum communication, **Quantum key distribution**. While using any messaging app with end-to-end encryption, to protect the messages sending to someone from prying eyes or eavesdropping, the app generates an encryption key using which the messages are encrypted and decrypted. This encryption key must be shared by both sender and receiver, the procedure by which the messaging app's backend gives both parties the encryption key is called key distribution. In classical key distribution,

whoever generates the key must find a way to send it to the other party. Nevertheless, how are we to trust that nobody else could intercept the distribution learn the key? The security of the sender's messages depends on the security of the sender's key distribution, and classically, there is no way to guarantee the security of the key distribution. With access to a quantum communication channel

1. BB84 Protocol

Suppose Alice wants to send Bob a message m without Eve being able to learn anything about its content.How can this be done? This can be achieved if Alice and Bob share in advance a string k of random bits. Alice computes $x = m \oplus k$ and send x to Bob. Eve cannot learn anything from x, But Bob can recover m by computing $x \oplus k$

$$(Pr(M = m|X = x) = Pr(M = m))$$

But this is not as simple as it seems. The main problem is that k has to be as long as m and cannot be reused so..... how to agree on k?

2. The Problem of Key Distribution

Alice and Bob may share several keys for later use when they are together.But if they cannot meet each other, there exist a key distribution method like Diffe-Hellman [7] protocol, but they are not unconditionally secure. Diffe-Hellman protocol can be broken with Quantum Computers. So there's a mojor problem of key distribution, which is solved by soemthing called Quantum Key Distribution.[8]

- **BB84: Alice's part**

In 1984, Charles Bennett and Gilles Brassard proposed the first protocol for Quantum Key Distribution (QKD)

Alice generates a private string of random bits. She could even do this with a quantum computer (H gate + measure) Then, for each bit, she randomly chooses if she encodes it in the $\{|0\rangle, |1\rangle\}$ basis or the $\{|+\rangle, |-\rangle\}$ basis. She can easily do this by using H and X gates.$(H|0\rangle = |+\rangle, H|1\rangle = |-\rangle, X|0\rangle = |1\rangle, X|1\rangle = |0\rangle)$ Alice sends the resulting qubits to Bob.

- **BB84: Bob's part**

Each time Bob receives a bit, he randomly decides whether he will measure it in the $\{|0\rangle, |1\rangle\}$ basis, or in the $\{|+\rangle, |-\rangle\}$ basis. He does this by applying the H or the NOT gate before measuring. He writes down the result and the basis he used, If he used $\{|0\rangle, |1\rangle\}$, he writes down 0 if he gets $|0\rangle$, and vice versa. If he used $\{|+\rangle, |-\rangle\}$, he writes down 0 if he gets $|+\rangle$ and 1 if he gets $|-\rangle$.

- **BB84: Alice and Bob on the phone**

After all this process, Alice and Bob talk on a classical channel(Authenticates but not necessarily secure)

Bob announces the bases he has used for the measurements, and Alice announces the bases she used to code.

Bob does not announce the result of his measurements.

For those bits in which Bob measures with the same basis that Alice used for coding, he has got the bit that Alice intended to send.

The rest are discarded (they will keep about half of the bits).

- **BB84: Eve tries to intercept and resend**

Imagine Eve has access to the qubits that Alice send to Bob.

Eve could try to measure and resend the qubit to Bob.

Eve cannot distinguish the four possibilities $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ because she does not know the basis that Alice has chosen. If Eve chooses a basis at random, she will error half of the time, and Alice and Bob may detect it. Eve cannot copy the qubits and wait to check the basis that Alice and Bob have used(no-cloning theorem) Other more complex attacks are possible but can be shown to fail.

With a classical channel, an eavesdropper Eve can copy the bits going to Bob without him finding out, The no-cloning theorem prevents her from doing the same in a quantum channel. Moreover, to learn any information about a qubit she has intercepted, Eve must make a measurement, which will alter the qubit state before Bob receives it. If Eve does make a measurement, then Bob's bits will not perfectly match Alice's bits, and so they will each have different keys. Since Alice and Bob will be using their respective keys to do further communication, they will quickly notice if their keys do not match, and they can find a new channel to generate a new key.

Check the code of BB84 on Github

B. The CHSH Game: Testing the Local Hidden Variable Theory

The CHSH inequality, which is named after John Clauser, Michael Horne, Abner Shimony, and Richard Holt[9], provides an experimental framework for supporting Bell's theorem, stating that the local hidden variable theories cannot precisely explain each and every quantum mechanical phenomenon, particularly entanglement. The inequality is derived with the assumption that hidden local variables exist, and it prescribes a constraint on the expected values of the Bell test experiment. Therefore, experimental violation of the CHSH inequality is evidence that there are no

local hidden variables. Here we describe the CHSH game, a hypothetical bell test experiment. The game players can use either classical strategies(corresponding to local hidden variable theories) or quantum strategies, which involve measurements of a shared entangled bit. It can be shown that quantum strategies allow a greater winning probability than classical strategies. These maximum probabilities correspond precisely to the CHSH inequality. Hence win frequencies under a quantum strategy appear to violate the maximal winning probability prescribed by classical formalisms.

Rules for the CHSH Game

Let Alice and Bob be spatially separated such that they cannot communicate. Suppose a referee sends a uniformly chosen bit x to Alice and a bit y to Bob. Alice and Bob then send bits a and b, respectively, back to the referee. They win if

$$a \oplus b = x.y$$

They can decide on a strategy beforehand, but they cannot communicate during the game.

There can be two startegies that Alice and Bob use:

- Classical Strategy
- Quantum Strategy

1. *Classical Strategy*

Let's break down the classical possibilities for this. The randomly generated bits could have the following values, and thus products:

- $x = 0$ and $y = 0$ so $x \cdot y = 0$
- $x = 0$ and $y = 1$ so $x \cdot y = 0$
- $x = 1$ and $y = 0$, so $x \cdot y = 0$
- $x = 1$ and $y = 1$ so $x \cdot y = 1$

On the other hand, the XOR logic options for the bits Alice and Bob will select can be as follows:

- $a = 0$ and $b = 0$ so a $\oplus$ b=0
- $a = 0$ and$b = 1$ so a$\oplus$b=1
- $a = 1$ and $b = 0$ so a$\oplus$b=1
- $a = 1$ and $b = 1$ so a$\oplus$b=0

The most optimal classical strategy for Alice and Bob is blatantly simple. Since $x.y$ produces 00 in 75% of cases, they should aim at producing 00 out of their a$\oplus$b operation too. This means that they should always output 00 or always 11, regardless of the input values of x and y – as long as they both stick to the same value all the time. This will ensure that $a \oplus b$ always results in 00,

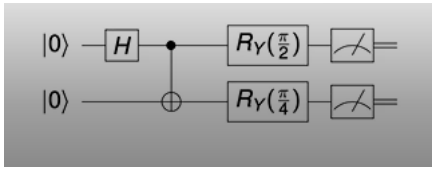

FIG. 3. The Circuit for CHSH Game

and since we already established that $x.y$ gives 00 in 3 out of 4 cases, they will also win the game 75% of the time. This is the best they can do classically.

Alice and Bob can win 75% of the time if they always answer $'0'$. No other deterministic strategy can do better and Probabilistic strategies are convex combinations of classical strategies, so they cannot improve the 75% success rate.

2. *Quantum Strategy*

With a quantum strategy, we allow Alice and Bob to share an entangled quantum state, although Alice and Bob themselves are still separated and cannot otherwise communicate.As it turns out, due to entanglement and the EPR correlations, quantum strategy can lead to a higher winning probability, namely 85%.

The Strategy

- Alice and Bob share a Bell pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ before the start of the game.
- If Alice receives 0, she measures her qubit and outputs the result.
- If she receives 1, she applies $R_Y(\frac{\pi}{2})$ to her qubit and then she measures it.
- If Bob receives 0, he applies $R_Y(\frac{\pi}{4})$. Else ,he applies $R_Y(-\frac{\pi}{4})$.
- Then he measures his qubit.
- The Probability of winning is now $cos^2(\frac{\pi}{8}) = 0.85$

It can be proved that $cos^2(\pi/8)$ is the highest possible success rate for a quantum strategy (Tsirelson's bound[10]). The CHSH game can be used to rule out local realism.

Code for CHSH game can be found on Github

C. SuperDense Coding and Quantum Teleportation

1. *SuperDense Coding*

Imagine a situation where Alice and Bob are in different parts of the world.

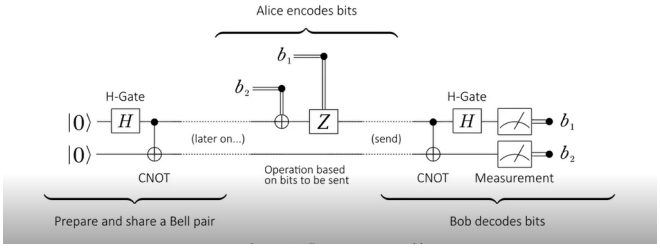

FIG. 4. SuperDense Coding

Alice has two bits: b_1 and b_2, that she wants to share or communicate with Bob, but only using one Qubit. So, she wants to encode two classical bits into a single qubit so that Bob, who is in the other part of the world, will recover the classical information. It turns out that there is no way she can accomplish this task without additional resources. However, let us imagine that a long time ago before Alice even knew what b_1 and b_2 are, that the two of them prepared two qubits A and B in the superposition.

Alice have the qubit A, and Bob have the qubit B. We can say that Alice and Bob share an entangled bit or an EPR pair.

It is natural to view entanglement as a resource as we will see; and when Alice and Bob each have a qubit, and the two of them are in the entangled state, it is natural to imagine that Alice and Bob share one unit (i.e., one entangled bit, or e-bit for short) of entanglement. Given the additional resource of a shared e-bit of entanglement, Alice will be able to transmit both a and b to Bob by sending just one qubit.

The SuperDense Coding Protocol: Alice's Part

- Alice and Bob share a bell pair in advance.
- Alice wants to send to Bob two classical bits b_1 and b_2
- If $b_2 = 1$, she applies X to her qubit
- If $b_1 = 1$, she applies Z to her qubit.
- Then she sends her qubit to Bob.

The SuperDense Coding Protocol: Bob's Part

- Bob receives Alice's qubit.
- He applies a CNOT gate controlled by Alice's qubit.
- He applies H to Alice's qubit
- He measures and recovers b_1 and b_2

Super dense coding : an example

Suppose Alice wants to send 11. We start with

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

After Alice's operations, we will have

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

When Bob applies CNOT he obtains

$$\frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle$$

And with the H gate he gets $|11\rangle$ that now he can measure.

Check the code for SuperDense coding on Github

2. *Quantum Teleportation*

Assume Alice has a qubit that she wants to send to Bob. $\alpha|0\rangle + \beta|1\rangle$ How many classical bits would be required to accomplish this task? The reasonable answer would be that no number of classical bits of communication will suffice. Alice may not know α and β

Moreover, there is no way for her to perform any measurements on her qubit that would unveil these numbers.

Thus, she could not tell this information to Bob because she was not able to determine it.

However, if we give Alice and Bob the additional resource of sharing an entangled bit, just as in superdense coding, it becomes possible for Alice to transmit a qubit to Bob using classical communication through quantum teleportation. Specifically, two bits of classical information will be needed to perform this task.

Quantum Teleportation: Alice's Part

- Alice and Bob share an entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- This can be done in advance or they can rely on a source that distributes entangled pairs.
- Alice applies a CNOT gate to the qubit she wants to teleport $|\psi\rangle = a|0\rangle + b|1\rangle$ and to her part of the bell pair. We will have

$$\frac{1}{\sqrt{2}}(a(|000\rangle + |011\rangle) + b(|110\rangle + |101\rangle))$$

- Alice further applies the H gate to the qubit she wants teleported. Then we have

$$\frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(b|0\rangle + a|1\rangle) + |10\rangle(a|0\rangle - b|1\rangle) +$$

$$|11\rangle(-b|0\rangle + a|1\rangle))$$

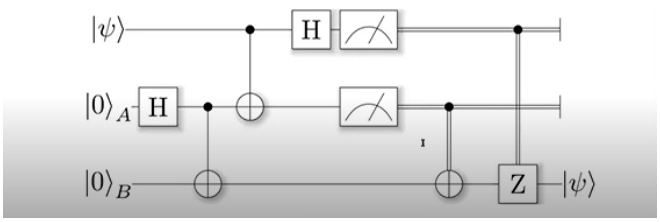

FIG. 5. Quantum Teleportation

- Alice measures her two qubits and sends the result(two classical bits) to Bob (through a classical channel)

Quantum Teleportation : Bob's part

- Bob uses the second bit received from Alice to decide if he applies X to his qubit.

- And he uses the first bit to decide if he applies Z.

It is not matter that is teleported but information. When Alice measure her qubit, she looses it(if not, we would be contradicting the no cloning theorem). To teleport a qubit, we need two classical bits and one entangled pair:

$$2bits + 1ebit \geq 1qubit$$

Teleportation is not instantaneous , we need classical communication Quantum teleportation has been shown experimentally (current record 1,400 km)

Check Simulation of Quantum Teleportation here.

III. PERSPECTIVE ON ITS USES

With the exponential growth in computing power, quantum computing is getting ready for its close up. Quantum Computers are ideal for solving complex problems, which are hard for classical computers but are easy to factor on a quantum computer. Such an advancement creates a world of opportunities across almost every aspect of modern life.

Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning are some prominent areas right now, as the emerging technologies have penetrated almost every aspect of humans' lives. Some of the widespread applications we see every day are in voice, image and handwriting recognition. However, as the number of applications increased, it became challenging for traditional computers to match up the accuracy and speed. Moreover, quantum computing can help in processing complex problems in very little time, which would have taken traditional computers thousands of years.

Cyber Security

The online security space is currently quite vulnerable due to the increasing number of cyber-attacks occurring globally daily. Although companies are establishing necessary security frameworks in their organisations, the process becomes daunting and impractical for classical digital computers. Moreover, cybersecurity has continued to be an essential concern around the world. With our increasing dependency on digitisation, we are becoming even more vulnerable to these threats. Quantum computing with the help of machine learning can help develop various techniques to combat these cybersecurity threats. Additionally, quantum computing can help in creating encryption methods, also known as quantum cryptography.

[0] Check the codes for the Quantum Algorithms on Github

[1] Leeuwen, Jan van, ed. (1998). Handbook of Theoretical Computer Science. Vol. A, Algorithms and complexity. Amsterdam: Elsevier. ISBN 0262720140. OCLC 247934368.

[2] Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of Statistical Physics. 22 (5): 563–591. Bibcode:1980JSP....22..563B. doi:10.1007/bf01011339. S2CID 122949592.

[3] Feynman, Richard (June 1982). "Simulating Physics with Computers" (PDF). International Journal of Theoretical Physics. 21 (6/7): 467–488. Bibcode:1982IJTP...21..467F. doi:10.1007/BF02650179. S2CID 124545445. Archived from the original (PDF) on 8 January 2019. Retrieved 28 February 2019.

[4] Manin, Yu. I. (1980). Vychislimoe i nevychislimoe [Computable and Noncomputable] (in Russian). Sov.Radio. pp. 13–15. Archived from the original on 10 May 2013. Retrieved 4 March 2013.

[5] Neumann, J. von (1956-12-31), "Probabilistic Logics and the Synthesis of Reliable Organisms From Unreliable Components", Automata Studies. (AM-34), Princeton: Princeton University Press, pp. 43–98, ISBN 978-1-4008-8261-8, retrieved 2020-10-10

[6] Wootters, William; Zurek, Wojciech (1982). "A Single Quantum Cannot be Cloned". Nature. 299 (5886): 802–803. Bibcode:1982Natur.299..802W. doi:10.1038/299802a0.

[7] Diffie, Whitfield; Hellman, Martin E. (November 1976). "New Directions in Cryptography" (PDF). IEEE Transactions on Information Theory. 22 (6): 644–654. CiteSeerX 10.1.1.37.9720. doi:10.1109/TIT.1976.1055638. Archived (PDF) from the original on 2014-11-29.

[8] Shannon, C. E. (1949). "Communication Theory of Se-

crecy Systems*". Bell System Technical Journal. Institute of Electrical and Electronics Engineers (IEEE). 28 (4): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x. hdl:10338.dmlcz/119717. ISSN 0005-8580.

[9] J.F. Clauser; M.A. Horne; A. Shimony; R.A. Holt (1969), "Proposed experiment to test local hidden-variable theories", Phys. Rev. Lett., 23 (15): 880–4, Bibcode:1969PhRvL..23..880C, doi:10.1103/PhysRevLett.23.880

[10] Boris Tsirelson (1987). "Quantum analogues of the Bell inequalities. The case of two spatially separated domains" (PDF). Journal of Soviet Mathematics. 36 (4): 557–570.