Learning with Quantum Computers

Soham Joshi
Computer Science and Engineering
IIT Bombay (of Aff.)
Mumbai, India
sohamjoshi@cse.iitb.ac.in

***Abstract*—Quantum Computing (QC), is a developing field with counter-intuitive and surprising results. Manipulating hidden information caused by the probabilistic nature of quantum information has enabled researchers to formulate algorithms with lesser asymptotic time complexity [1]. Moreover, the combination of hidden information and entanglement at the quantum level has led to the reformulation of several machine learning algorithms in the language of quantum computing [2]. This survey presents some of the basic concepts needed to understand quantum computing and quantum information, and covers some of the machine learning algorithms which have been optimized due to this field.**

***Index Terms*—Quantum Machine Learning, Quantum Computing, Quantum Information**

I. Introduction

This report is a part of the project, "Machine Learning with Quantum Computers" [3], under the guidance of Siddhant Midha and Aditya Sriram. The project is a part of a program named "Winter in Data Science" (WiDS) conducted by Analytics Club, IIT Bombay. In this paper, basic concepts of quantum computing and quantum information will be covered in a way that is accessible to the reader with a knowledge of basic linear algebra and some quantum mechanics. In this report I will also survey some research papers pertaining to the fields of quantum machine learning (QML). Additionally the project includes implementation of quantum algorithms using qiskit and pennylane, the code for which can be found here. This paper is meant to be an overview of QC, so some parts of this paper may leave facts without proof. In such cases, kindly refer [2] for more details.

II. Quantum bits

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, or qubit for short. Note that a bit is just a mathematical entity, in physical circuits high/low voltages can be modelled by a bit taking value 1 or 0. Analogously a qubit is just another abstract mathematical entity. Does this mean that the qubit isn't "real"? Yes, a qubit is a tool used for modelling quantum mechanical systems. But studying the properties of the qubit is still worth our time since this helps us to develop a theory independent of physical constraints and which helps model reality to a good approximation.

A. States of a qubit

Just as a bit can take values 0, 1; a qubit can be in states $|0\rangle$, $|1\rangle$. Moreover, a qubit can be in a linear combination of these states given by :

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

where $\alpha, \beta \in \mathbb{C}$.
The state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as the computational basis states [1], form an orthonormal basis for this vector space. But, what makes a qubit different from a bit? It is the fact that the coefficients of linear combination α, β cannot be measured. Quantum mechanics tells us that we can obtain much more restricted information about this state, particularly, upon measurement, we can obtain $|0\rangle$ with probability $|\alpha|^2$, and $|1\rangle$ with probability $|\beta|^2$. Since the probabilites must sum to 1, the restriction $|\alpha|^2 + |\beta|^2 = 1$ is imposed on the coefficients of linear combination.

B. Bloch sphere

A tool which helps to visualise actions on a qubit is known as the *Bloch sphere*. Because of the restriction imposed on $|\alpha|, |\beta|$, we can rewrite the state of a qubit as :

$$|\psi\rangle = e^{i\gamma}\left(cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle\right)$$

In the next section we will see that global phase factors have no effect so this can be re-written as :

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

C. Multiple qubits

Suppose we have two qubits. If these were two classical bits, then there would be four possible states, 00, 01, 10, and 11. Correspondingly, a two qubit system has four computational basis states [2] denoted $|00\rangle, |10\rangle, |10\rangle, |11\rangle$. A pair of qubits can also exist in superpositions of these four states,

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

[1] Measurement can be done with respect to a basis other than this. For instance, measurements can be done with respect to the basis $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle \equiv \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

[2] Another example of commonly used basis are called the "bell states/EPR pairs", given by $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}; |\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}; |\beta_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}; |\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$

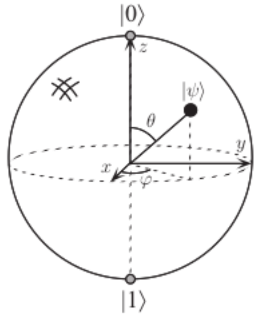


Fig. 1. Bloch sphere representation of a qubit

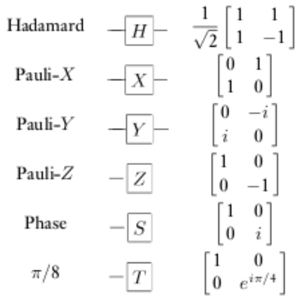
Similar to the case for a single qubit, the measurement result x (= 00, 01, 10 or 11) occurs with probability $|\alpha_x|^2$, with the state of the qubits after the measurement being $|x\rangle$. More generally, we may consider a system of n qubits. The computational basis states of this system are of the form $|x_1 x_2 ... x_n\rangle$, and so a quantum state of such a system is specified by 2^n amplitudes.

III. Quantum Gates

Classical gates are responsible for manipulating bits, essentially representing a boolean function from bits to bits. Similarly, quantum gates are just a function from qubits to qubits. In this section, we shall explore the different classes of quantum gates. We will not delve into proofs but offer an operational description of how quantum gates work. Further details for this can be found in V

A. Single-Qubit gates

A qubit can be written as a 2×1 unit vector in the space spanned by $|0\rangle, |1\rangle$. So, a transformation from a single qubit to another qubit transforms a unit vector to another unit vector. Hence, it follows that all quantum gates are unitary. Moreover, it turns out that any unitary operation is a valid quantum gate and can be constructed from some "universal" quantum gates (will be discussed later).



Hadamard
H
$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X
X
$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y
Y
$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z
Z
$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase
S
$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$
T
$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

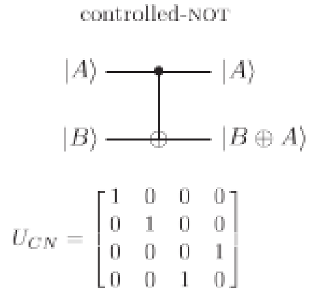
Fig. 2. Single qubit gates

Some single qubit quantum gates are shown in figure 2. Since we are dealing with the qubit as an abstraction, a quantum gate is just a black box operator that performs a unitary transformation to a qubit. For now, we will not deal with the question of the physical realisation of these gates.

B. Multiple qubit gates

In classical computation, there are five notable quantum gates, namely NOT, AND, OR, NAND, NOR. As it turns out, all of these gates can be simulated using quantum gates as well. But, as a first step, consider the controlled-NOT, or the CNOT gate (figure 3). Now, we go into an important point when dealing with quantum gates. Even though the circuit diagram shows two input lines in the circuit, the CNOT gate doesn't act on a single qubit, but a system of two "entangled" qubits. Hence, the only correct way to apply the circuit is to take the tensor product of the two input vectors, apply the gate and obtain another tensor product. The notation $|a\rangle \otimes |b\rangle$ is often abbreviated as $|a\rangle|b\rangle$ or $|ab\rangle$. So the action of a gate U will be given as :

$$|a\rangle|b\rangle \xrightarrow{U} U|a\rangle|b\rangle$$



controlled-NOT
$|A\rangle$
$|A\rangle$
$|B\rangle$
$|B \oplus A\rangle$
$U_{CN} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

Fig. 3. CNOT gate

Moreover, just because the control qubit does not change values when it is a computational basis state doesn't mean that it will remain the same for all vectors. In fact, the control qubit often changes and measuring it's state is a key step in several quantum algorithms. Another important fact is that any multiple qubit quantum gate can be constructed using CNOT and single qubit quantum gates. Hence, they form a set of universal quantum gates. So, the CNOT gate is analogous to the XOR gate, but not exactly equivalent. Can gates be constructed exactly equivalent to NAND, XOR gates? Turns out this is not possible because quantum gates must be reversible whereas XOR and NAND gates are irreversible, i.e., given the output of these gates, the input cannot be uniquely identified.

C. Quantum circuits

We have already seen some quantum circuits, but let us examine quantum ciruits in some more detail. Each line in the circuit is represented by a wire, but this wire is not necessarily physical, it may as well represent the passage of time, or a physical particle such as a photon. There are a few features allowed in classical circuits that are not usually present in quantum circuits. Loops in a circuit are not allowed, FANOUT and FANIN operations are not allowed. This is because of the "no-cloning"[3] theorem. An example of a quantum circuit is the "quantum teleportation circuit"(figure 4). The setting of the problem is that Alice and Bob met long ago but now live far apart. While together they generated an EPR pair, each taking one qubit of the EPR pair when they separated. Alice now wants deliver a qubit $|\psi\rangle$ to Bob. She does not know the state of the qubit, and moreover can only send classical information to Bob. This can be achieved using the circuit given.

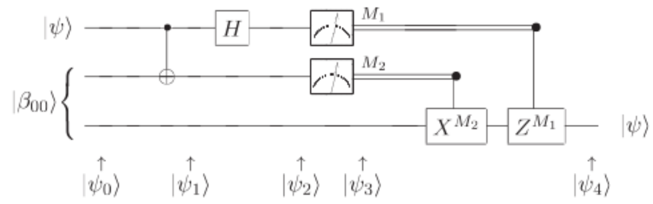
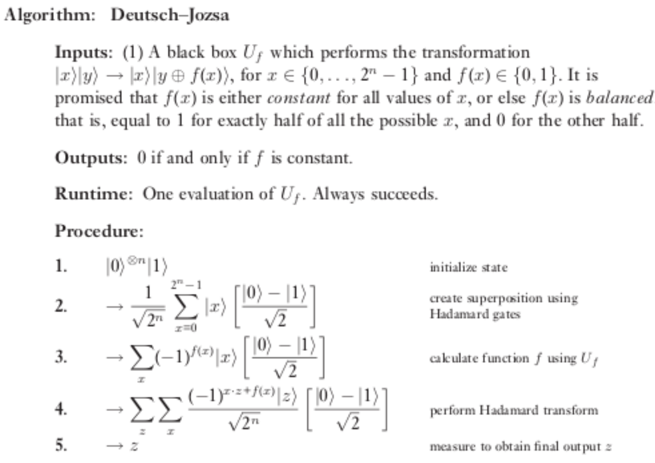


Fig. 4. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits)

D. The Deutsch-Jozsa algorithm

The problem is as follows. Alice, selects a number x from 0 to $2^n - 1$, and mails it in a letter to Bob. Bob calculates some function $f(x)$ and replies with the result, which is either 0 or 1. Now, Bob has promised to use a function f which is of one of two kinds; either $f(x)$ is constant for all values of x, or else $f(x)$ is balanced, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half. Alice's goal is to determine with certainty whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible. In order to solve this we use the algorithm described (figure 5). The circuit for the same is shown in figure 6



Algorithm: Deutsch–Jozsa

Inputs: (1) A black box U_f which performs the transformation $|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$, for $x \in \{0, \ldots, 2^n - 1\}$ and $f(x) \in \{0,1\}$. It is promised that $f(x)$ is either *constant* for all values of x, or else $f(x)$ is *balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs: 0 if and only if f is constant.

Runtime: One evaluation of U_f. Always succeeds.

Procedure:

1. $|0\rangle^{\otimes n}|1\rangle$ initialize state
2. $\to \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ create superposition using Hadamard gates
3. $\to \sum_x (-1)^{f(x)} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ calculate function f using U_f
4. $\to \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ perform Hadamard transform
5. $\to z$ measure to obtain final output z

Fig. 5. Deutsch-Jozsa algorithm

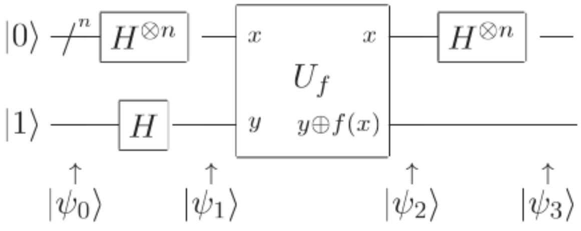


Fig. 6. Deutsch-Jozsa algorithm's circuit

Finally, if the measurement yields all 0s then the function is constant, otherwise balanced. The reader can try verifying this as an exercise.

IV. The postulates of quantum mechanics

Quantum mechanics is a mathematical framework for the development of physical theories. Just as newton's laws are axioms for classical mechanics, the postulates of quantum mechanics are not "derived", but assumed. The motivations of these postulates(axioms) may not always be clear, since they have been guessed after a lot of experimentation. So, this part of the report aims at knowing the postulates and gaining an operational understanding of the same. Understanding these axioms will help us realise what happens in physical systems, and not the abstract vectors we have been dealing with till now.

A. State space

Postulate 1 : Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

Quantum mechanics does *not* tell us, for a given physical system, what the state space of that system is, nor does it tell us what the state vector of the system is. Figuring that out for a specific system is a difficult problem for which physicists have developed many intricate and beautiful rules. We will take the qubit as our fundamental quantum mechanical system.

B. Evolution

Postulate 2 : The evolution of a *closed* quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi^{'}\rangle = U|\psi\rangle$$

Just as quantum mechanics does not tell us the state space or quantum state of a particular quantum system, it does not tell us which unitary operators U describe real-world quantum dynamics. Quantum mechanics merely assures us that the evolution of any closed quantum system may be described in such a way. Another interesting result follows from this postulate. If t_1 and t_2 are "close", then we can talk about derivative of functions,

[3] The no-cloning theorem states that "qubit-copying" is not permitted. Hence, junctions of wires are not permitted in a quantum circuit. The no-cloning theorem proves to be useful in quantum encryption protocols like BB84 [4]

Postulate 2' : The time evolution of the state of a closed quantum system is described by the Schrödinger equation

$$i\hbar\frac{d}{dt}|\psi\rangle = H|\psi\rangle$$

In this equation, $\hbar$ is a physical constant known as Planck's constant whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor $\hbar$ into H, effectively setting $\hbar = 1$. H is a fixed Hermitian operator known as the Hamiltonian of the closed system[4].

C. Quantum measurement

Even though the internal evolution of a quantum system can be worked out, there are times when we need to measure the quantum system, i.e. interact it with the experimental set-up which leads to the system not being closed anymore. This postulate addresses this development of the system.

Postulate 3 : Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|psi\rangle$ immediately before the measurement then the probability that result m occurs is given by,

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle$$

A simple but important example of a measurement is the measurement of a qubit in the computational basis. This is a measurement on a single qubit with two outcomes defined by the two measurement operators $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. The probability of measured outcomes can be verified using this postulate.

An important application of Postulate 3 is to the problem of distinguishing quantum states. In the classical world, distinct states of an object are usually distinguishable, at least in principle. For example, we can always identify whether a coin has landed heads or tails. An important result follows from postulate 3 that only only *orthogonal states* can be distinguished.

D. Composite systems

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle\otimes|\psi_2\rangle\otimes\cdots\otimes|\psi_n\rangle$.

Further details about density operators, EPR can be found in [2].

V. Quantum circuits

In this section, we will examine some more circuits and gates, theorems that help us to construct more complicated gates from simple building blocks.

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the rotation operators about the $\hat{x}, \hat{y}$, and $\hat{z}$ axes, defined by the equations:

$$R_x(\theta) \equiv e^{\frac{-i\theta X}{2}} = cos\frac{\theta}{2}I - isin\frac{\theta}{2}X$$
$$R_y(\theta) \equiv e^{\frac{-i\theta Y}{2}} = cos\frac{\theta}{2}I - isin\frac{\theta}{2}Y$$
$$R_z(\theta) \equiv e^{\frac{-i\theta Z}{2}} = cos\frac{\theta}{2}I - isin\frac{\theta}{2}Z$$

Theorem : (**Z-Y decomposition for a single qubit**) Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_x(\delta)$$

A. Controlled operation

Controlled operations.

Acknowledgement

I would like to thank the mentors of this project Siddhant Midha and Aditya Sriram for giving me the opportunity to study and appreciate this subject.

References

[1] M. Schuld, I. Sinayskiy and F. Petruccione, "An introduction to quantum machine learning," September 2014.

[2] M. Neilson and I. Chuang, "Quantum Computing and Quantum Information, 10th edition"

[3] S. Midha and A. Sriram "Learning with Quantum Computers" *Github repository*, January 2023.

[4] C. H. Bennett, G. Brassard "Quantum cryptography: Public key distribution and coin tossing" March 2020.

[4] Earlier, we spoke about applying a unitary operator to a system. Doesn't this contradict the fact that postulate 2 only holds for closed systems? Yes! We should consider the experimentation set-up as a part of our system if we want to use the hamiltonian to describe it. But, the unitary operator is a good enough approximation that we can push this nuance under the rug.