Qubit, Quantum Entanglement and all that: Quantum Computing Made Simple

Zion Elani[a)]

Institute for Nanotechnology and Advanced Materials, Bar-Ilan University, Ramat-Gan, 5290002 Israel

(Dated: 31 January 2020)

QUANTUM computing, a fancy word resting on equally fancy fundamentals in quantum mechanics, has become a media hype, a mainstream topic in popular culture and an eye candy for high-tech company researchers and investors alike. Quantum computing has the power to provide faster, more efficient, secure and accurate computing solutions for emerging future innovations. Governments the world over, in collaboration with high-tech companies, pour in billions of dollars for the advancement of computing solutions quantum-based and for the development of fully functioning quantum computers that may one day aid in or even replace classical computers. Despite much hype and publicity, most people do not understand what quantum computing is, nor do they comprehend the significance of the developments required in this field, and the impact it may have on the future. Through this lecture notes, we embark on a pedagogic journey of understanding quantum computing, gradually revealing the concepts that form its basis, later diving in a vast pool of future possibilities that lie ahead, concluding with understanding and acknowledging some major hindrance and speed breaking bumpers in their path.

Keywords: quantum computing, quantum mechanics, superposition, entanglement, decoherence, qubit, quantum logic gates

[a)]zion.elani@biu.ac.il

CONTENTS

I. INTRODUCTION

When we contemplate finding the prime factors of a number, we do not give the slightest thought to how this seemingly simple process can turn out to be a persistent computing problem. Yes, this is not a mistake! The solutions can be easily reached for numbers up to a certain limit, whereas the process becomes increasingly demanding in terms of time and space for conventional-classical computers. It would take months, years, centuries, millennia and even longer than the age of the universe itself, for a classical computer, to solve such a problem despite the fast-growing processing power. This prime factorization is the basis of many cryptographic algorithms such as RSA since no algorithm has been known to efficiently and fast factor all integers. Numerous such real-life cases emerge, like in molecular modeling and mathematical optimization, where conventional computers fail to do their magic. This is where quantum computing comes into the picture. But before investigating further the concepts of quantum computing, we must discuss the fundamentals of classical computing. The limitation imposed on conventional computers is their very foundation. Conventional computers use bits to store and process data. These bits are either in a state of ON or OFF, 0 or 1. Computers make use of transistors to process data/information in the form of sequences

of various combinations of those 0s and 1s. Grouping those transistors into special circuits is called logic gates, and allows the computer to calculate and make decisions following man-made computer programs. The computer processing power depends on the number of transistors used. Since that infrastructure spans those definitive states of 0s and 1s, it cannot be applied by way of exploring the endless possibilities offered by various problems in nature, possibilities that follow the laws of quantum mechanics.

To grasp the complexity of the issue, let us consider the example of molecular modeling. Currently, the world's most powerful supercomputers cannot simulate a molecular system consisting of more than a few hundred atoms. This inability persists since electrons exist at once in a multiplicity of states, a concept called superposition. This number, a mere few hundreds, is not at all huge. For example, an average-sized protein macromolecule contains a string of approximately 400 amino acid molecules whose mean number of atoms per amino acid is around 20. Quantum computers, as opposed to classical ones, leverage the fact that they operate using the concept of superposition.

These concepts in quantum computing will be discussed in detail in the coming sections. The purpose of these notes is to pedagogically unveil the mysteries of apparent complex concepts in quantum computing to layman's eyes. In the coming sections, we will first introduce a brief history of quantum computing, gradually progressing toward the explanation of the basic working principle of quantum computers and eventually discussing and arriving at various concepts such as superposition, entanglement, etc., applying a simple, easy to understand approach. Our aim, while writing these notes, has been to keep the readers from being overwhelmed by complex routes of explanations as given by experts in this field. Hence, these notes represent non-expert writing that allows the reader to feel connected and in-level with the content of this article.

II. BRIEF HISTORY

Considering that the majority of phenomena and processes in the universe are quantum in nature, the need for quantum computing is ever increasing. However, this need was not fully acknowledged until 1981, when Nobel laureate Richard Feynman pointed out in a conference that computing based on classical logic could not easily and efficiently process calculations describing quantum phenomena. Feynman considered the possibility of comput-

ing that could potentially operate in a quantum manner, the same as nature itself. Feynman concluded his lecture "simulating Physics with Computers," saying *"I'm not happy with all the analyses that go with just the classical theory, because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly, it's a wonderful problem, because it doesn't look so easy. Thank you."*[1,2].

Meanwhile, in 1980, Paul Benioff,[3] an American physicist and one of the pioneers of quantum computing working on quantum information theory, came up with the first quantum mechanical computing model, thus paving the way for the theoretical possibility of quantum computers. Later on, in 1985, David Deutsch, a British physicist at Oxford University, suggested a way to mathematically understand the possibilities that lie in quantum computers.[4,5]. In 1994, the interest in quantum computing dramatically rose when Peter Shor developed a quantum algorithm to efficiently find the prime factors of large numbers.[6]. A cascade of developments in quantum computing followed. In 1998, in an attempt to solve a problem posed by Deutsch, Jonathan A. Jones, and Michele Mosca at Oxford University experimentally demonstrated the first working 2-qubit NMR quantum computer.[7]. Later, various high-tech companies such as Microsoft and IBM became involved in the development of quantum computing solutions. In January 2019, IBM unveiled its first commercial 20-qubit quantum computer under the name IBM Q System One.[8]. in October 2019., IBM's yet another and biggest quantum 53-qubit computer went online. Not only that, but following the publication of its research in Nature,[9], Google announced in October 2019 that it has achieved quantum supremacy after its 54-qubit Sycamore processor was able to perform a calculation in 200 seconds. In the past, such a calculation would have required $10,000$ years of a standard supercomputer. We have thus demonstrated how increasing global investment in quantum computing makes the future seem brighter and full of possibilities.

III. QUANTUM SUPERPOSITION, ENTANGLEMENT AND DECOHERENCE

In the quantum world, a state of a system, for example, an electron or an atom, is described by a state vector referred to as a wave function. A probabilistic interpretation of the wave function that describes the state of a system under investigation is used to explain various quantum effects such as finding the system in a particular state. The fact

that a wave function can describe microscopic particles has a relation to the wave-particle duality, a concept revealing that energy and matter can exhibit both wave and particle properties. This concept demonstrates the failure of classical concepts, such as "particle" or "wave", to elucidate the phenomena observed on small-scale objects. A particle, such as an electron, can feature a wave property (in addition to its momentum and position properties) to represent what is known as an electron wave function. Likewise, the wave function of light can be attributed to particle properties such as momentum and position, hence the concept of a photon.[10,11] When two waves pass through a point in space, they superpose to form a common wave height (amplitude) at the same point depicting the sum of the two wave amplitudes - a phenomenon called interference. Likewise, in the microscopic world, any quantum states can be superposed, i.e., added together to yield another valid quantum state. This principle, called quantum superposition, means that a quantum state can be represented as a sum of other distinct states. Any physical system in the quantum world may be represented in one of many configurations, each specified by a complex number, whereas the most general state of the system is a combination of all these possibilities.[11]. Quantum mechanics tells us that the state of a quantum particle can only be known when one of its physical properties is measured. According to the Copenhagen interpretation of quantum mechanics, valid only in the microscopic world, we cannot show the physical properties of a system being investigated before it being measured, and the only prediction possible is the probability of a given measurement possible. Furthermore, the act of measurement affects the system. Performing a measurement on the system results in the collapse (i.e. reduction) of the system's set of probabilities to only one of its possible values. In quantum mechanics jargon, this feature is termed "wave function collapse."

Schrödinger, who opposed this interpretation, sought to illustrate the absurdity of the notion that the laws of nature change in the transition from subatomic systems to macroscopic systems. In his famous thought experiment devised in 1935, Schrödinger proposed a scenario wherein a cat is placed in a steel box along with a Geiger counter, a vial of poison, a hammer and a radioactive substance. Once the radioactive substance decays, the Geiger counter is impacted and triggers the hammer to release the poison, which eventually kills the cat. According to quantum mechanics theory, the radioactive atom can either decay or not at any given moment. There's no telling of its decay exact moment, but once it does decay, it is sure to break the vial, release the poison and kill the cat. Before performing a

measurement, then, quantum mechanics tells us that the radioactive substance and the cat are in a superposition of being non-decayed/dead and decayed/alive. Until the box opens, an observer has no way of knowing whether the cat is alive or dead in response to the radioactive substance decay. Being a random process, the death of the cat is hard to predict. This leaves the cat, until observed, both "living or dead in equal parts". Oddly, then, before the measurement, i.e., until the system collapses into one configuration, the cat exists in a peculiar superposition state of being both alive and dead.[12]. Quantum computing works on a similar premise. The state of a quantum bit (qubit) in computing can be, until observed, in $|1\rangle$ or $|0\rangle$ at the same time (here we introduce the notation $|1\rangle$, $|0\rangle$ for the quantum states). All quantum computations are performed when the qubit is in a superposition state. Once it collapses to either of the definitive states, it loses its quantum nature and starts behaving as a classical bit.

Entanglement is another counter-intuitive quantum phenomenon, according to which a pair or a group of particles in superposition are entangled (interwoven). For example, the result of the measurement of one qubit will always be correlated to the measurement of another qubit even if the particles are separated from one another by a large distance. If the quantum state that represents the physical system cannot be factored as a product of states of its local constituents, we say that the quantum system is entangled. This means that in an entangled quantum system one constituent cannot be fully described without considering the other constituents of the system as well.

Since the wave function describes the probability of the particle, say of an electron being in space and time, it usually refers to a point in space and time when the electron is discovered. For example, the detection of the electron by a particle's detector. The reality of the collapse of the wave function is debatable, raising the question of whether it is a physical process in itself or rather a secondary phenomenon of another quantum process, such as quantum decoherence. Quantum decoherence is the way to describe the interaction of a quantum system with its environment. This interaction, which, loosely speaking, can be called "measurement", causes changes in the system that resemble the collapse of the wave function.[10]. In physics, a phase is a concept that describes the momentary state of a periodic wave. It is the place in the period where the wave is in a certain state. Wave coherence is the extent to which wave phase differences remain constant. This property allows the waves to form a stationary interference pattern. If both waves are periodic and

have the same frequency, the wave's amplitude at the point of intersection depends on the difference between the waves' phases: some phase differences will experience constructive interference; others will experience destructive interference. But if the frequencies of the two waves are not perfectly matched, the difference in phase between them will change in time, and so will their interference pattern. It can thus be concluded that coherence is a property of waves that maintains a definite phase difference between them over time. In optics, for example, a coherent source in time is a source that radiates waves of the same frequency in the same initial phase or waves whose phase difference is fixed. Monochromatic light, for example, contains only one frequency and therefore emits coherent waves. This contrasts with a non-coherent source where the difference between the waves is random.

In the microscopic world, a quantum system is coherent if it is not interwoven with its surroundings, so it can be found in a superposition of several states that can intertwine. If between different states there is a definite phase relation, the quantum system is said to be coherent. Once the system responds to its environment in such a way that each state of the system has a corresponding state of the environment, and where the environmental states do not overlap, it can be said that the environment "measured" the system and that the system lost its coherence. This process of loss of coherence is called quantum decoherence. As a result, quantum behavior is lost, just as kinetic energy appears to be lost by dint of friction forces in classical mechanics (which results in a transfer of energy into thermal energy).

Quantum decoherence can stem from several experimental factors such as the finite life-times of the quantum states, experimental noises in the system or through environment interaction. An example of decoherence can be found in the double-slit experiment: when a beam of particles, say electrons, passes through two slits and then hits the screen, an image of the interference pattern is reflected on the screen. The interference pattern is created when particles passing through the upper slit take a different path from those passing through the second slit, thus accumulating a different phase. The accumulated phase determines, once the particles hit the screen, whether the interference is constructive or destructive. However, a measurement made to determine through which of the slits the particles went through before reaching their destination, i.e. the screen, will cause the particle wave function collapse and destroy the interference pattern. Hence, the measurement itself causes decoherence. Even a partial measurement that does not cause a complete collapse of the particle wave function will cause the phases to mix and thus gradually disrupt the interference pattern.

The decoherence not only destroys the superposition and reduces it to a particular state (location in our experiment), it also destroys the ability of the individual states from being able to interfere with each other. This concept of decoherence is vital in quantum computation as it dictates the preservation of coherence of states and complete management of decoherence, in order to practically perform quantum computation (for entangled qubits, their states cannot be described independently of each other). The slow progress in the practical application of quantum computing is due in large part to quantum coherence, which causes difficulty in maintaining a quantum interconnected state. As a result of interaction with the environment, quantum states tend to very quickly lose the relative phases that characterize them and receive random phases.[10,13,14]. Quantum computers perform calculations while the wave function is in superposition states. This superposition allows the calculations performed to simultaneously use state 1 and state 0. As we explained before, while performing a measurement, decoherence occurs and the wave function that represents the superposition of the quantum system state collapses into one particular state. Nevertheless, such a performance is problematic: to be able to read the computational results, a non-stop continuation of calculations performance will be required before a new measurement can be made. Since the very nature of the measurement process is probabilistic, a quantum computer returns a non-deterministic final result. Such random output requires the use of particular algorithms. In addition to that, one should bear in mind that, as opposed to classical computing, quantum computing requires an algorithm design exclusive/specific to a particular problem.

IV. QUBITS AND EXPONENTIAL GROWTH

As mentioned earlier, quantum computers are fundamentally different from the classical ones. The basic unit of operation in quantum computers is a qubit, i.e., a quantum bit.[13–15]. Qubits have special properties: they can exist in superposition, i.e., in a state of "on" and "off", represented simultaneously by either notation, $|0\rangle$ and $|1\rangle$ and may be entangled thus sharing physical properties despite being apart. In this state of superposition, the qubits have the probability of being a $|0\rangle$ or being a $|1\rangle$. The Bloch sphere, depicted in fig.(1), facilitates a better visualization, with the poles representing classical bits. These are the only two possible states of a classical bit representation. However, qubits cover the whole

sphere benefiting from the vast possibilities of states, thus making room for an abundance of information. As a result, when a qubit is measured, it collapses to one of the two poles $|0\rangle$ or $|1\rangle$. The collapse direction, i.e. the determination of pole to which the qubit collapses, depends on the direction the arrow points to. For example, if the arrow is closer to the south pole, it is highly probable the qubit will collapse to the south pole and vice versa. This probability corresponds with θ, the angle between the pure state on the sphere (represented by the vector) and the vertical z-axis (see fig.(1)). Further, by changing the angle φ, the vector rotates with respect to the z-axis. This rotation will only change the phase of the quantum state; it will not change the probability by which the vector collapses to one or the other state after the act of measurement.

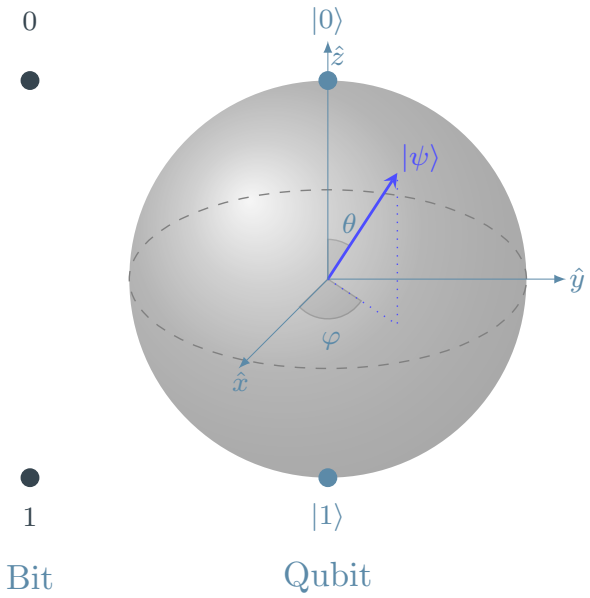

FIG. 1. A sphere representing the state of a single qubit $|\psi\rangle$. Unlike a classic bit, which can be in either state, that is 0 or 1, a qubit can be in a state $|0\rangle$, $|1\rangle$ or in a quantum superposition of states and may be entangled with other qubits. Quantum measurement is a probabilistic process and its result depends on the measurement base. After performing a measurement, the state of the qubit is destroyed in a process known as the collapse of a wave function and what remains is an entirely classical answer - which of the two basis states of the qubit was measured ($|0\rangle$ or $|1\rangle$).

Let us slow down to appreciate how these qubits give us speed and processing advantage over classical bits. Since qubits can exist in between the states $|0\rangle$ and $|1\rangle$, they introduce numerous possibilities of problem-solving. Moreover, the computing power of quantum

computers increases exponentially with the number of qubits. In other words, the effect of superposition becomes more pronounced once we scale up from a 1-qubit system to a N-qubit system. Fig.(2) represents the famous wheat-chessboard problem (the myth of the invention of chess), displaying how exponential growth is extremely powerful. Impressed by the chess game presented to him by its inventor, the emperor of India asked the inventor to name his reward. Whereupon the inventor named his humble reward (or so the emperor thought) in the form of one wheat grain on the first square of the chessboard followed by its doubling each day on each subsequent square of the 64 squares. The naive emperor, amazed at this modest request, granted him his wishes. After a week or so, the treasurer informed the emperor that the reward would add up to a huge number, far greater than the total wheat production of the whole empire for years to come. By doubling the number on each subsequent square, the number of grains seems to increase gradually on the first squares but soon increases as to appear almost infinite. The increase follows the formula of 2^{n-1} grains on the n square which results in over a million grains of wheat on the $21st$ square and reaching more than ten to the twelfth power (10^{12}), a trillion, on the $41st$ square. Although there are only 64 squares on the chessboard, such a tremendous growth poses a demand that will not be satisfied even by the world's entire wheat crop .[16].

Extrapolating this mythical demand to our problem, in a 2-qubit system, the possibilities to reach a solution increase by 2^2. Likewise, it increases to 2^3 for a 3-qubit system, 2^5 for a 5-qubit system, eventually reaching 2^N for a N number of a qubit system. For a 300-qubits system we find a superposition of 2^{300} states. This mind-boggling 91 decimal digit number (2 novemvigintillion...) is more than the number of atoms in the visible universe ($\approx 10^{82}$)! Thus, a slight increase in the number of qubits can lead to a rapid increase in computing power, eventually leading to a faster and efficient information processing than conventional computers. In other words, the computational power increases exponentially with an increase in the number of qubits. A single qubit can hold up to 2-bits of information. However, the full computational power stems from using many qubits: for a system of N-qubits, a complete specification of its quantum state requires 2^N complex numbers which are far more than the description of a classical N-bit system which requires only N bits.

Let us review what we have said so far. Superposition tells us that a qubit can simultaneously exist in both states 0 and 1 before that outcome. It is also true that after the act of measuring the qubit state, the qubit will be in only one particular state, 0 or 1, no different

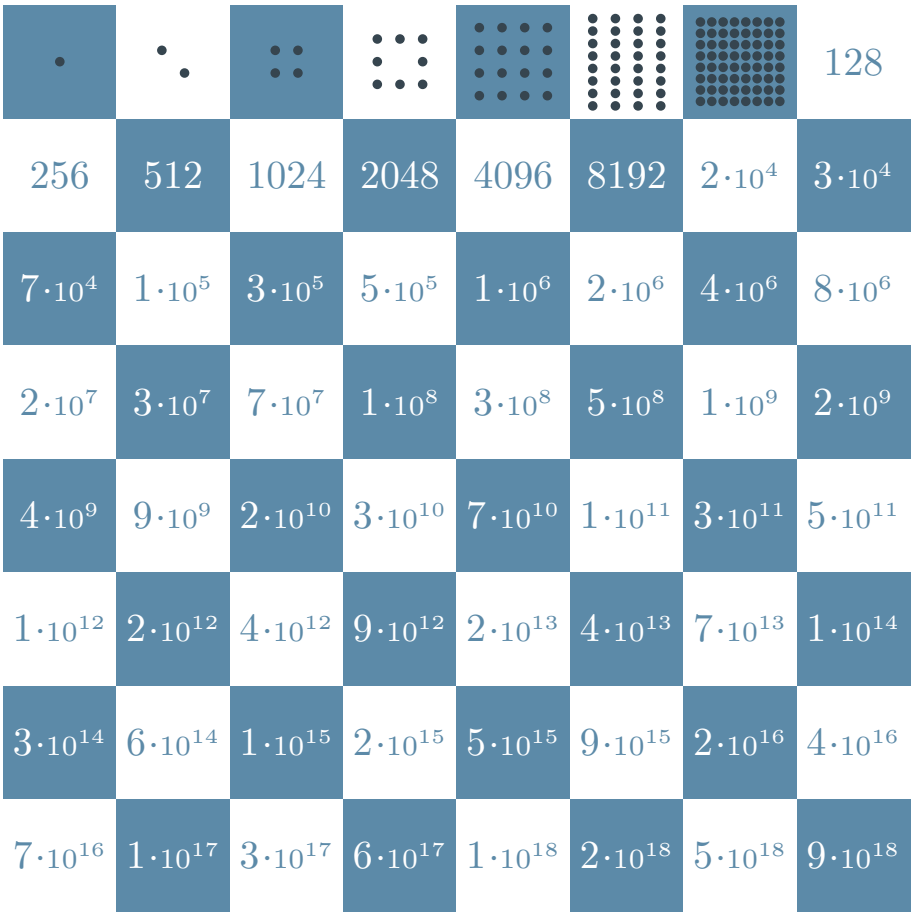

FIG. 2. Chessboard representing an exponential increase in the number of grains as we move up the checkers: by doubling the number on each subsequent square, the number of grains seems to increase slowly on the first squares but soon increases swiftly as to appear almost infinite.

from a bit in a classical computer. The difference derives from the fact that in between measurements the quantum computer is at one and the same time in a superposition of both 0 and 1. What about 2-bits (2-qubit) systems? In a classical computer, 2-bits can represent one of 4 possible states: the state 00, the state 01, the state 10, or the state 11. Importantly, we have to remember that 2-bits can be in only one of these 4 possibilities at a time. This is not the case for qubits in quantum computers. 2-qubits indeed have 4 states representation as classical 2-bits, but due to superposition, 2-bits in a quantum computer can represent all 4 states at the same time. Practically, we can think of it as if 4 classical computers operate together. But what happens when we add more bits to our classical computer, say N-bits? As we explained above, a classical computer will be in only one state at a time. However, adding more qubits to a quantum computer, say, N-qubits, results in exponential growth

of the computing power since N-qubits can simultaneously represent 2^n states. A classical N-bits system can be in *only one* state out of the 2^N possible permutations (Fig.3), while a N-qubits system can be *in all* of the 2^n possible permutations (Fig.4). Let us illustrate this by considering a particle passing through a maze. While passing through this confusing intricate network of passages, we can think of the particle as being at the same time in a superposition of all the paths. This occurs as a result of the particle following the quantum superposition principle. The analogy of a quantum particle in a maze is akin to how parallel computing works, where multiple processing elements are simultaneously carried out to solve a problem by splitting the task between the processors to get results faster than serial processing. Seth Lloyd's succinctly described the difference between classical and quantum computation by saying: *"A classical computation is like a solo voice—one line of pure tones succeeding each other. A quantum computation is like a symphony—many lines of tones interfering with one another."*[17]

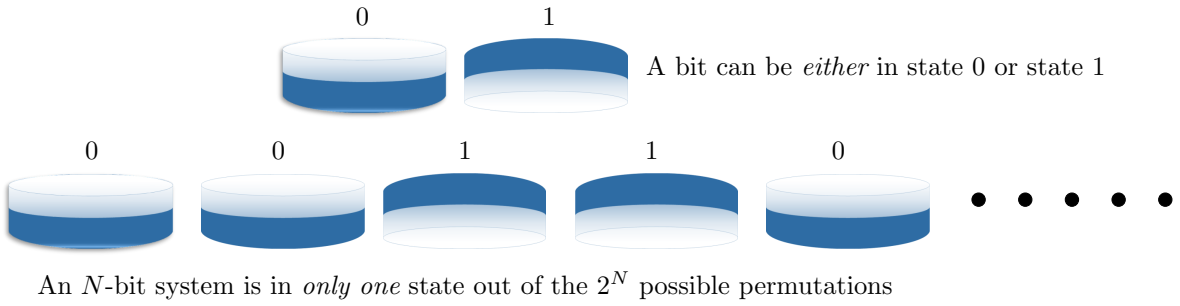

FIG. 3. An illustration of bits as checkers A classical. A classical bit can be *either* in state 0 or state 1 (first row). An N-bits system can be in *only one* state out of the 2^N possible permutations (second row).

V. QUANTUM LOGIC GATES

A bit in our every-day computers, laptops, and smartphones is a component of the computer memory (usually) represented by an electrical DC voltage or current pulse, to which only two modes are required, "*on*" (1 = *electric current*) and "*off*" (0 = *no electric current*). The bit takes the values of 1 and 0 based upon the algorithms provided by a computer program. For a qubit in a real quantum computer, we can have different physical realizations. A qubit can be realized as an electron with spin, semiconducting loops, trapped ions, a

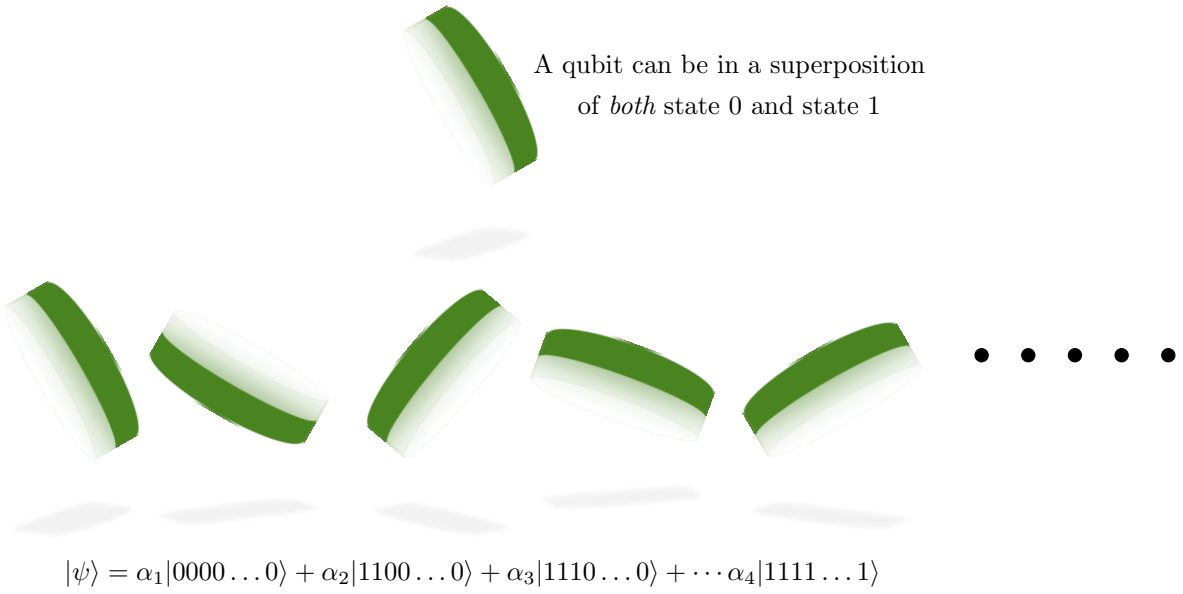

FIG. 4. An illustration of qubits as checkers. A qubit can be in a superposition of *both* state 0 and state 1. An N-qubits quantum system can be *in all* of the 2^n possible permutations:
$|\psi\rangle = \alpha_1|0000\ldots0\rangle + \alpha_2|1100\ldots0\rangle + \alpha_3|1110\ldots0\rangle + \cdots \alpha_4|1111\ldots1\rangle$

polarized photon, or as diamond vacancies to name a few. Based on these realizations, one can implement a quantum computer, though it is yet unclear which implementation will be best applied in the future.

Before exploring the concept of quantum logic gates, let's first try to understand what a logic gate is. A logic gate is any system of a physical structure that accepts a set of binary inputs and gives out a single binary output. They are the basic building blocks of any digital system. The input corresponds with a certain output based on a certain logic. This logic is applied through logic gates. The main logic gates at the base of digital circuitry of classical computers are AND, OR, NOR, NAND XOR, XNOR and NOT. For example, the AND gate returns an output as 1 (ON) only when both binary inputs are 1 (ON) whereas the OR gate returns 1 (ON) even when one of the two binary inputs is in 1 (ON). Another classical gate takes one bit as an input and returns a single bit with revered value. All these gates collectively work to form a digital circuit that operates based on a set of algorithms.

Likewise, quantum computing operates on certain logics executed through quantum gates. These quantum gates work with qubits to generate a possible solution. But unlike classical logic gates, quantum gates are reversible.[14] By saying that quantum gates are reversible

we simply mean that, in principle, they never lose information. Conversely, classical gates in every-day computers lose information which means, among other things, that ordinary computers cannot retrace their steps (at least not currently[18]). In other words, an entangled qubit continues to be entangled after leaving the quantum gate. What this means is that the information it carries will continue to be sealed. These reversible quantum gates are represented by unitary matrices (a unitary matrix is a matrix whose inverse equals its conjugate transpose). The most common quantum gates operate on one or two qubits, described by 2×2 or 4×4 matrices respectively with orthonormal rows. We briefly introduce these logic gates below (for further details refer to the books listed in the bibliography):

- Hadamard gate: This gate is used to create a superposition between $|0\rangle$ and $|1\rangle$.
- Pauli-X: Analogous to classical NOT gate. It transforms $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. It is equivalent of rotating $|\psi\rangle$ around the x-axis to π radian (180 degrees).
- Pauli-Y: Represents the rotation of $|\psi\rangle$ around y-axis to π radian. It transforms $|0\rangle$ to i$|1\rangle$ and $|1\rangle$ to -i$|0\rangle$.
- Pauli-Z: Represents the rotation of $|\psi\rangle$ around y-axis to π radian. It transforms only $|1\rangle$ to $-|1\rangle$ and has no effect on $|0\rangle$.
- Phase shift gate: It is the generic gate that represents all the phase shift gates including the Pauli-Z gate.
- Controlled gate: These gates are multiqubit gates that require at least 1-qubit as control and one qubit as a target. The gate will operate on the target qubit only if the control qubit is in a particular state.
- Toffoli gate: Universal reversible logic gate. It is also known as a controlled-controlled-not gate. These gates are the building blocks of any reversible circuits.

VI. FUTURE OF QUANTUM COMPUTING

With the capacity to efficiently process gazillion amounts of information in just a few seconds, quantum computers have a potentially bright future ahead. Some of their many computing advantages will be felt in the fields of cryptography, molecular modeling for

designing new drugs and materials, financial modeling, weather forecasting and change, machine learning and artificial intelligence, traffic optimization among many more. We must bear in mind that quantum computers will not replace the classical ones. The two will simply co-exist because quantum computers are designed to solve a particular set of problems that a classical computer will not be able to unravel. It will be disadvantageous economically while less efficient to employ quantum computing resources for simple day-to-day tasks. Rather, quantum computers will supplement classical ones by dealing with complex problems in far less time.

As mentioned earlier, the large number factorization problem, which forms the basis of modern cryptography, would be easily solvable within a few seconds thus jeopardizing the current RSA encryption systems. However, thanks to the new type of highly secure cryptography offered by quantum mechanics, keeping up and even developing better encryption systems will be in the realm of the possible. The phenomenon of entanglement will further assist in the process. For example, party A, say Alice, wants to send some information to party B, Bob, through a secured key distributed via quantum key distribution (QKD), which randomly enables the distribution of key. In such a state of affairs, Alice will receive half of the entangled qubit pairs while bob will receive the other half. Since the qubits distributed between them are entangled, i.e., highly correlated, once Alice and Bob measure these qubits, their results will be one and the same. In other words, they will get the same string of ones and zeros from the measurement of those entangled qubits. Should an eavesdropper attempt to spy on this signal, the key at Bob's end will no longer be the same as Alice's as a result of the system being disturbed and compromised during transmission. As long as Alice and Bob keep receiving data while their key is long and similar, they can be sure that their information has not been compromised. This is how quantum computing will contribute to better secure transmission of information.

Another way quantum technology can help in the future is made clear when we look at the structure of atoms. Electrons in an atom exist as an electron cloud representing the probability distribution of their position. The very nature of these electrons is highly quantum and the simulation of the interactions between various atoms and molecules cannot be made using classical computations. The use of quantum computing will enable a deeper exploration of these interactions and design better drugs and materials for various applications. Recently, the auto industry has become interested in improving car batteries using

this technology. The German car manufacturer Daimler AG has partnered with Google and IBM to explore the possibilities of how quantum computing can potentially supercharge AI.[19]. Another car manufacturer giant, Volkswagen, has teamed up with D-wave systems to run pilot programs on their quantum computing systems to study traffic optimization problems using Beijing, Barcelona, and Lisbon as traffic models.[20]

Yet another supremacy of quantum computing will be felt in the prediction of weather. It will enable way easier, accurate and faster weather predictions compared to the results produced by supercomputers currently employed for the task. According to researchers at Rigetti computing, *"Harnessing [quantum computers' statistical distribution] has the potential to accelerate or otherwise improve machine learning relative to purely classical performance"*.[21] *"I think AI can accelerate quantum computing"*, Google CEO Pichai said, *"and quantum computing can accelerate AI"*. Thus, quantum computing and machine learning will move ahead hand-in-hand.[22]

The potential of quantum computing is vast and with the current pace of development and advancement, it is hard to anticipate what quantum computers will be able to accomplish in the future. Unfortunately, for now, one of the hindrances to quantum computing development is the lack of infrastructure required for the realization of a fully functioning quantum computer that can take over the current computing scenario. Quantum computers are extremely difficult to engineer, build and program. Moreover, two major hurdles challenging the realization of fully functioning quantum computers are decoherence and the measurement of the output of quantum computers. As we explained earlier, decoherence is the loss of coherence, i.e., loss of the state of superposition due to interactions with the external disturbances caused by vibrations, temperature fluctuations, electromagnetic waves and other interactions with the outside environment. Building perfect qubits is a challenge to current engineering as it is very difficult to isolate them from the external environment to prevent them from decohering. Such engineering involves building superconducting circuits to maintain extremely low temperatures. Furthermore, it is also important for the quantum gates to act on qubits before the qubits decohere. Another problem is to make qubits behave entangled. There have been developments to correct the loss of entanglement known as quantum fault tolerance. Indeed, quantum error correction techniques do exist, however, they consume such a large number of qubits that relatively very few numbers of qubits are left for actual computation. Yet another major problem with quantum computing is found

in the attempt to measure its output. The practical application of quantum computers will require the measurement of the state of a qubit, rendering it decohered while the output is any random state of its infinite possible states. Let's consider 100-qubits in the state of superposition. Measured, their coherence will be lost, and we will get one of the random states of a qubit out of the random states of 99-qubits. This random state may or may not be the correct answer. To rectify this, amplitudes of probabilities are created and assigned to each state and algorithms that manipulate the amplitudes. These algorithms are aimed at making the amplitudes that fall towards the wrong answer cancel each other out and the ones falling in the correct path be in phase with each other. This way, when we measure the state, the superposition collapses in the amplitude with the highest probability, thus giving the correct answer. The development of these algorithms is no cakewalk. Most of the algorithms today have been designed to solve a particular set of problems with a very limited scope of operation. Thus, we are today in a very primitive stage of quantum age.

VII. SUMMARY

Through these notes, we explored the vast potential of quantum computing while understanding the basic concepts of quantum mechanics such as superposition, entanglement, and decoherence that form the basis of operation in a quantum computer. These concepts were introduced in a pedagogical way for an amateur enthusiast to easily understand. We introduced the basic unit of computation in a quantum computer, qubits, along with the basic workings of the logic gates that operate on those qubits. We also flashed various possible applications of quantum computing and discussed how it will solve the problems currently unsolvable or less efficiently solvable by contemporary computational solutions. Furthermore, we acknowledged various limitations and difficulties in the way of fully utilizing the power of quantum computing.

REFERENCES

[1]F. R., "Tiny Computers Obeying Quantum Mechanical Laws. Talk delivered at Los Alamos National Laboratory," *New Directions in Physics: The Los Alamos 40th Anniversary Volume*, 1983. [Online]. Available: https://lib-www.lanl.gov/lascience27.shtml

[2]R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6-7, pp. 467–488, Jun. 1982. [Online]. Available: https://doi.org/10.1007/bf02650179

[3]P. Benioff, "The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *Journal of Statistical Physics*, vol. 22, no. 5, pp. 563–591, May 1980. [Online]. Available: https://doi.org/10.1007/bf01011339

[4]D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 400, no. 1818, pp. 97–117, Jul. 1985. [Online]. Available: https://doi.org/10.1098/rspa.1985.0070

[5]S. Akama, *Elements of Quantum Computing*. Springer International Publishing, 2015. [Online]. Available: https://doi.org/10.1007/978-3-319-08284-4

[6]P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press. [Online]. Available: https://doi.org/10.1109/sfcs.1994.365700

[7]J. A. Jones and M. Mosca, "Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer," *The Journal of Chemical Physics*, vol. 109, no. 5, pp. 1648–1653, Aug. 1998. [Online]. Available: https://doi.org/10.1063/1.476739

[8]"IBM Unveils World's First Integrated Quantum Computing System for Commercial Use," 2019. [Online]. Available: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use#assets_all

[9]F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick,

A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019. [Online]. Available: https://doi.org/10.1038/s41586-019-1666-5

[10]J. Audretsch, *Entangled World: The Fascination of Quantum Information and Computation*. Wiley, 2008. [Online]. Available: https://books.google.co.il/books?id=DlfJIl24xpkC

[11]T. Norsen, *Foundations of Quantum Mechanics*. Springer International Publishing, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-65867-4

[12]G. Auletta and S. Wang, *Quantum Mechanics for Thinkers*. Pan Stanford, 2014. [Online]. Available: https://books.google.co.il/books?id=Xc2uAwAAQBAJ

[13]J. Cramer, *The Quantum Handshake: Entanglement, Nonlocality and Transactions*. Springer International Publishing, 2018. [Online]. Available: https://books.google.co.il/books?id=tHWutQEACAAJ

[14]M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. [Online]. Available: https://books.google.co.il/books?id=-s4DEy7o-a0C

[15]"Introduction: A New Quantum Revolution," 2019, NIST, National Institute of Standards and Technology Web site. [Online]. Available: https://www.nist.gov/topics/physics/introduction-new-quantum-revolution

[16]C. Pickover, *The Math Book: From Pythagoras to the 57th Dimension, 250 Milestones in the History of Mathematics*, ser. Sterling Milestones Series. Sterling, 2009. [Online]. Available: https://books.google.co.il/books?id=Z22NuQAACAAJ

[17]S. Lloyd, *Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos*. Knopf Doubleday Publishing Group, 2006. [Online]. Available: https://books.google.co.il/books?id=vcExCDmVn-0C

[18]M. P. Frank, "Throwing computing into reverse," *IEEE Spectrum*, vol. 54, no. 9, pp. 32–37, Sep. 2017. [Online]. Available: https://doi.org/10.1109/mspec.2017.8012237

[19]"The next big thing?" 2018, Magazine for Mobility and Society. [Online]. Available: https://www.daimler.com/magazine/technology-innovation/quantum-computers-future-daimler-google-ibm-technology.html

[20] "Volkswagen to Test Quantum Navigation App in Real Traffic," 2019, the Wall Street Journal. [Online]. Available: https://www.wsj.com/articles/volkswagen-to-test-quantum-navigation-app-in-real-traffic-11572553300

[21] J. S. Otterbach, R. Manenti, N. Alidoust, A. Bestwick, M. Block, B. Bloom, S. Caldwell, N. Didier, E. S. Fried, S. Hong, P. Karalekas, C. B. Osborn, A. Papageorge, E. C. Peterson, G. Prawiroatmodjo, N. Rubin, C. A. Ryan, D. Scarabelli, M. Scheer, E. A. Sete, P. Sivarajah, R. S. Smith, A. Staley, N. Tezak, W. J. Zeng, A. Hudson, B. R. Johnson, M. Reagor, M. P. da Silva, and C. Rigetti, "Unsupervised machine learning on a hybrid quantum computer," 2017. [Online]. Available: https://arxiv.org/abs/1712.05771

[22] "Google CEO Sundar Pichai on achieving quantum supremacy," 2019, MIT Technology Review. [Online]. Available: https://www.technologyreview.com/s/614608/google-ceo-quantum-supremacy-interview-with-sundar-pichai/