Quantum Computing. An approach to Quantum Supremacy

by Sergio Alejandro Sotres Romero

December 10th 2019

Contents

Abstract

The main goal of this project is to discuss the main features of Quantum Computing and to inform about the achivements to reduce the Quantum Supremacy gap. In the first part of the manuscript the reader will explore the basic concepts under the current behaivour of Moore's law. Later on, some historical background of the research and the implementation of both software and hardware is presented, so the reader can identify the differences between a classical and a quantum system in computation. The discussion continues with some applications and the role of quantum supremacy nowadays. Finally, some final remarks about the topic along with some concerns about the possible ethical repercussions of working with quantum computers are mentioned.

1 MOTIVATION

Nowadays, people are used to see the increase of capacity and power on computers year after year. These tremendous changes can be observed with the new models of smartphones, personal computers, smart watches coming up to the market making that any user of those devices formulate an immediate question such as: How far is it possible to increase the computational power of such devices? or Is there a limit of what one can do with them? To understand the reason of why mankind has been able to do such computational improvement in the past decades, it is useful to first understand how computers are built.

All computers available in the market are based on a collection of integrated circuits. This means that the main structure of the computer is based on a collection of different electromagnetic circuits connected to each other in a specific way to perform the task the user is demanding at the computer. These integrated circuits consist on a bunch of transistors which basically are conducting lines of electric current. Such flow of electricity can be interpreted as a certain task for a part (or the entire) circuit, to perform the task the user asks. What's interesting about the way computers are built, is the set up and architecture of such collection of transistors which is related to the number of elementary units the integrated circuit actually has. In other words, one can be able to perform more complex calculations if the number of elementary physical units (transistors) available increases. The latter because it is possible to manipulate the process of conducting electric current in specific conducting lines creating in that way 2 states: State "on" (meaning that the electric current is present. Typically represented with 1) and state "off" (meaning that the electric current is NOT present. Represented with 0). In this way, very modern techniques have been developed over the decades to optimize the process of electric flux for the machine to perform calculations and also to encode and storage the information that it produces. With all of this in mind, how many transistors can one place in an integrated circuit?

1.1 Creating smaller chips

To answer the question above, first it's worth to say that in recent days is very common to think that computer speed doubles every 18 months (approximately). If computers consist of a bunch of integrated circuits, then it must mean that the number of transistors available play an important role for increasing the computational speed in the recent years.

In 1965 the Co-founder of Intel Gordon Moore, predicted that the number of transistors will double every 18 to 24 months. The prediction was so accurate that up to this day, any smartphone has more computing power that NASA when they put two men on the moon. Moore's prediction more commonly known as Moore's Law, has been very accurate for approximately 50 years but according to some researchers (like as physicist Michio Kaku), claim that calculations based on Moore's law predict that the computing power around 2020 will be so powerful that the usual silicon chips (transistors) will not be able to conduct enough energy to keep up. The reasons to that is when the chips are approximately 20 atoms across (like a Pentium chip layer), silicon technology has problems with heat and leakage. The first is a thermodynamical problem because the heat reached by the chip will make it melt and the second one is because at that scale, Quantum Mechanics takes over for the behavior of electrons at the chip making a difficulty for performing more complex calculations.

To be more pragmatic regarding this matter, Moore's law has started to slow down from doubling every two years to doubling three years instead. The reason to this is due to miniaturization. Obstacles such as the speed of light, the atomic nature of materials and a molecular level workspace in parallel with the growing cost; has made experts, researchers and technology leaders to seek for alternative procedures to deal with such obstacles in order to keep increasing the computational power.

To put things in perspective regarding miniaturization, a microprocessor incorporates the feature of a CPU on a single integrated circuit, which as mentioned before, consist of a bunch of transistors. Up to this day a CPU is a microprocessor with billions of transistors. Another example that demonstrate how far Moore's law have becaome nowadays, is the first microprocessor from Intel (4004) which consisted of approximately 2,300 transistors of 10 μm. If compared to a single transistor on the mass market on 14 nanometers (the smallest reach 1 nm), we see that Intel has packed over 100 million transistors on each square milliliter. A true miniaturization.

With that in mind, if silicon-based technology is reaching its limits, is it possible to find alternative solutions? There are a number of proposals: protein computers, optical computers, molecular computers, DNA computers and one of the most trending of all: quantum computers which is the main topic of the essay. At this point it is estimated that advances in computing will evolve to quantum computing, a revolutionary technology that uses atomic particles to power computer processors.

It is important to remark that quantum computing does not go in parallel with the phrases DNA computing or optical computing.The latter describe the ingredient or substrate on which computation is done without changing the notion of computation, typically known as Classical Computation (i.e. using usual chips or transistors). Classical computers just like the ones we all have on our desks, make use of quantum mechanics, but they compute using bits, not qubits (the elemntary piece if information of a quantum computer). This means that the physical system to compute is still classical. Whether the computer is quantum or classical depends on how the information is represented and manipulated. That means in a classical or quantum way. When the phrase quantum computing is used in this manuscript, one has to remember that the two profiles differ greatly. In fact, classical computing does not present entanglement, a key component for quantum computation.

2 BASIC CONCEPTS OF A QUANTUM COMPUTER

In order to start exploring about Quantum Computing, first we must ask us the following question: What is a quantum computer and how are they different from the classical ones? To answer these questions it is convenient to give the following definitions:

Definition. A **quantum computer** is a device that leverages specific properties described by quantum mechanics to perform computation.

The definition above means that a classical computer can be described by quantum mechanics since quantum theory is the basis of the physical universe that we observe. But despite that a clssical computer can be described by the use of quantum mechanics, it does not works nor takes any advantage of the specific properties that quantum mechanics affords when doing its calculations.

For a typical laptop, it is possible to think of such as a *classical math machine* and is because it woks with *bits* that vary between 1 and 0 (*i.e* classical bits), which represent a single number in a calculation.These bits are sequences of 1,0 that physically represents whether electrical current IS or IS NOT present in the circuit respectevely. In other words, whether the switch is On or OFF. But quantum computers use quantum bits (also denoted as: *qubits*), which can exist as 1 and 0 at the same time. A superposition of the states 1 and 0 (Normally written in Dirac's notation as $|1\rangle$, $|0\rangle$). This feature that qubits work in a superposition state is very helpful because it tells us that the pieces of information sometimes are in $|1\rangle$, some others in $|0\rangle$ and some others in any number between $|0\rangle$,$|1\rangle$. Therefore, instead of only working with two dicrete states, they can operate so many numbers simultaneously.

According to the principles of quantum mechanics, systems are set to a definite state only once they are measured. In other words, before a measurement is done to the system, there are in an indeterminate state. But after the measure is performed, they are in a definite state. If we have a system that can take on one of two discrete states when measured, we can represent the two states in Dirac notation as $|0\rangle$ or $|1\rangle$ just like is written above. Therefore, a *superposition of states* is a linear combination of such states and is written as

$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle \tag{1}$$

With this idea in mind, we can give the following definition:

Definition. The superposition Principle is referred when a linear combination of two or more state vectors is actually another state vector in the same *Hilbert Space* (an abstact mathematical space) and describes another state of the system. Putting it in other terms, any element of thr Hilbert space can be written as a linear combination of the basis terms.

To exemplify superposition we can think of a propierty of light called *polarization*. The light that one sees on a daily basis has no preference direction for the polarization. Therefore, polarization states can be selected by using a *polarizing filter*, that is a thin film with an axis that only allows light with polarization parallel to that axis to pass through.

With a single polarizing filter, we can select one polarization of light, for example vertical polarization, which we can denote as $|\uparrow\rangle$ and the horizontal polarization denoted as $|\rightarrow\rangle$. Therefore, any polarization state $|\psi\rangle$ can be written as a linear combination of the basis states.

$$|\psi\rangle = \alpha\left|\uparrow\right\rangle + \beta\left|\rightarrow\right\rangle \tag{2}$$

Here the coeficients α and β represent complex numbers denoted as *amplitudes*.

One of the fathers of Quantum Theory, Max Born [1] demonstrated that the modulus squared of the amplitudes of a state is the probability of that state resulting after the measurement. Such probability has to be normalized and in this way, it enables to relate a connection between the amplitdes to the probabilities of the measurement with the Born rule:

Definition. The Born Rule states that in a superposition of states, the modulus squared of the amplitude of a state, is the probability of that state resulting after measurement. So, for the state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ the following condition must be satisfied: $|\alpha|^2 + |\beta|^2 = 1$, where α, β are complex numbers.

The Born Rule leads a critical difference between classical and quantum mechanics because the amplitudes (not the *probabilities*) can now be complex instead of just real numbers. Notice that up to this point we can see that Quantum Mechnics (QM) is a discipline where common sense and classical intuition is lost to some extend given the fact that in order to observe the system, we must measure it given the fact of the probabilistic nature of the quantum system. In 1935 Einstein, Podolsky and Rosen (EPR) published a paper [2]on quantum entanglement which showed that if one takes two entangled particles and then measure one of them, this automatically generates a correlated state of the second regardless of the distance between them; this was the seemingly illogical result that EPR hoped to use to show that QM itself must have a flaw. This is a cornerstone in Quantum Mechanics and has opened a very rich field in research nowadays. What this means is that entanglement happens when a supperposition of states is present on the study system and cannot be separable. With this concept in mind it is possible to define the following:

Definition. Quantum Entanglement refers when two or more systems are in a special case of superposition. If the measurement of one system is correlated with the state of the other(s) such that correlations between them are stronger than in the classical sense, then we refer that propierty as entanglement. In other words, the states of the system(s) are not separable.

Now that we have defined the superposition principle and the Born rule, let's mention the concept of irreversibility first introduced by Landauer in 1961. In his paper [3], he asked about *The ultimate physical limitations on the search for a faster ans more compact computing circuits.* That is, Does it exist a lower bound to the energy dissipated in the process of a basic unit of computation? Thanks to Landauer and others, it is now believed that it is in fact a limit (known as Landauer's Bound (LB)). To exemplify this we can think of the energy cost of erasure of n bits is $nkT\ln(2)$ where 4k is the Boltzmann constant, T is the temperatutre in Kelvin. This limit is the minumum amount of energy dissipated for an irreversible computation. Landauer defined logical irreversibility as a condition in which *the outcome of a device does not uniquely define the inputs.* He then claimed that *logical irreversibility...in turn implies physical irreversibility, and the latter is accompanied by dissipative effects.* The latter comes from the second law of thermodynamics which states that the total entropy of a system cannot decrease and, more specifically, must increase with an irreversible process [4].

With this in mind, the notion of *reversibility* plays an important role, because if one limits to operators with reversible gates then we do not loose information during the measurement. In other words, information cannot be lost no matter the process we ecounter.

Definition. Reversibility of Quantum Computation means that all operators in QC other than for measurement must be reversible.

As mentioned before, a *bit* is the basic unit of information for computational porposes, but because now we are interested on considering the quantum nature, then a *qubit* is basically a quantum bit. A quibit can take the states 0 or 1 but while in general a two-level system is used to build quantum computer, it is possible to choose other types of computational architectures. For instance, one could build a QC with *qutrits* which are a three-level systems. To create a better notion of what this entails, let's think of a qubit system of 100 qubits. That means we are thinking of 2^{100} states (approx 1.26 x10^{30}), while a qutrit system can handle 3^{100} states (approx 5.15 x10^{47}), a number 17 orders of magnitude larger. Since it is more difficult to build qutrit systems, following the mainstream in QC, this manuscript will only refer to quibits. It is why it is convenient to give the definition of such concept.

Definition. A Qubit is a two-level quantum system that can be mathematically represented as an entity that lives in a two-dimensional complex Hilbert space, $\mathbb{C}^2$.

If we think for instance about the states in equation (1), we can represent such states as vectors in the state space, which have the following matrix form:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3}$$

Any state in QC can be represented as a vector that begins at the origin and terminates on the surface of the unit Bloch sphere (Figure 1). We can identify the the two states $|0\rangle$, $|1\rangle$ at the diametral poles of such sphere, and any linear combination of them represented by any point on the surface of it. Notice that the so-called unit Bloch sphere is unitary to mantain the probability under control.

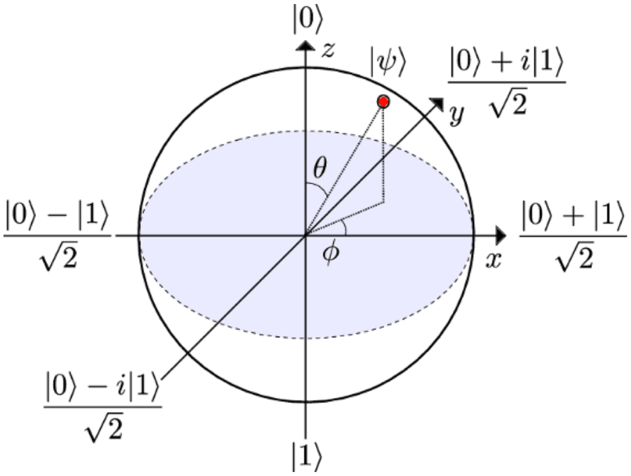
$|0\rangle$
z
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
y
θ
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
ϕ
x
$\frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
$|1\rangle$

Figure 1: The Bloch sphere taken from [5]

3 BACKGROUNG OF QUANTUM COMPUTING

Quantum computers and quantum information were a process slowly developed in the 1980s and early 1990s. Nevertheless, before those decades some researchers were concerned about the quantum nature in computation. Paul Benioff in 1979 [23] gave the theoretical basis for quantum computing and suggested that such computer could be built. Couple years later people such as Benioff, Manin and Richard Feynman (the latter one who argued that a classical system could not adequately represent a quantum mechanical system [7] in a lecture entitled *Simulating Physics with Computers*); set the features that a quantum implementation of a computer have to be useful. Opening the doors to a new generation of modern physics dedicated to research the algorithms that a Quantum computer should have.

During 1985 in Oxford, David Deutsch suggested a more comprehesive framework for quantum computing [8] where he describes what a quantum algorithm would look like. Later on he developed an algortihm that would run faster on a quantum computer developing a notion of a quantum mechanical Turing machine. Daniel Bernstein, Vijay Vazirani, and Andrew Yao then improved Deutsch's model and showed that a quantum Turing machine could simulate a classical Turing machine and therefore, any classical computation, with at most a polynomial time slowdown. It is how the standard quantum circuit model was then defined, ledding to an understanding of quantum complexity in terms of a set of basic transformations called *quantum gates*. The idea of a gate can be thought as the number of procedures or *steps* that a state must have to end up in another state.

By the 1990s, the first quantum algorithms were developed. Regardless of the probabilistic nature of quantum mechanics, the first quantum algorithms, for which superiority over classical algorithms could be proved, give the correct answer with certainty. They improve classical algorithms by solving in polynomial time with certainty a problem that can be solved in polynomial time only with high probability using classical techniques. In 1993 Bernstein ans Vazirani published a paper where they describe an algorithm that showed clear quantum-slassical separation allowing small erros. This is important because although Deutsch-Jozsa showed a deterministic quantum advantage, if small errors are introduced in the computation, the quantum and the classical versions can be run at $\mathcal{O}(1)$ steps, which means that there is no difference at all. In contrast, Bernstein algorithm showed that separation exist even when small errors are allowed. Such result is of no direct practical interest, since the impossibility of building a perfect machine reduces any practical machine running any algorithm to solving a problem. But such results were of high theoretical interest, since they showed for the first time that quantum computation is theoretically more powerful than classical computation for certain computational problems.

The latter results were useful for various researchers such as Peter Shor, who in 1994, developed a polynomial-time quantum algorithm for factoring large integers into two prime factors. This result provided a solution to a well-studied problem of practical interest. Factoring large numbers is a very hard problem and is the core of public key cryptography (PKG) as implemented in the RSA algorithm, that kind of cryptography is the basis of most all communications today over the internet. It goes from securing credit card numbers to online message systems. It is unknown whether an efficient classical solution exists, so Shor's result does not prove that quantum computers can solve a problem more efficiently than a classical computer.

Despite the fact that Shor's result gives an interesting outcome for the implementation of a quantum algorithm, there are some doubts about its practicalllity. To mention some, one can think of the fact that quantum systems are very fragile, menaing that they can easily be destroyed by external conditions like temperature and pressure. Also, inconveniets like the presence of decoherence in entangled states given by enviromental influences creates some doubts whether to believe that the idea of quantum computing is even possible. Properties of quantum mechanics, such as the impossibility of reliably copying an unknown quantum state, made it look unlikely that effective error-correction techniques for quantum computation could ever be found. For these reasons, it seemed unlikely that reliable quantum computers could be built.

Despite the ups and downs, researchers kept exploring the field and in 1996 Shor and Robert Calderbank, and independently Andrew Steane, saw a way to seemingly show-stopping problems of quantum mechanics to develop quantum error correction techniques. Today, quantum error correction is one of the most mature areas of quantum information.

During the years, there have been strong limitations on the power of quantum computation because for many problemsit does not provide any significant advantage over classical computation. After Shor, Lov Grover contributed with the creation of the other major algorithmin the mid-1990s. It provides a small speedup for unstructured search algorithms. Grover's algorithm achives only quadratic speedup, not exponential (like Shor's). But depsite that, quadratic speedup means that in an algorithm would be of order $\mathcal{O}(N)$ in the number of steps on a classical computer, then it is possible to achieve the same goal in $\mathcal{O}(\sqrt{N})$ steps on a Quantum computer. Grover's search algorithm applies to unstructured search. For other search problems, such as searching an ordered list, quantum computation provides no significant advantage over classical computation. Simulation of quantum systems is the other significant application of quantum computation known in the mid-1990s. Of interest in its own right, the simulation of increasingly larger quantum systems may provide a bootstrap that will ultimately lead to the building of a scalable quantum computer.

While some people were making progress with the agorithms that would run on a quantum computer, with a significative speedup over the classical ones, some other researchers were making progress on the physical implementation. In 1999-2001 Nakamura [10], [11] used Josephson junctions to create a two-level system that the user could manipulate between its two states, which opened up the field for investigating superconducting qubits. Another approach for implementing a quantum computers was proposed by Cirac and Zoller in 1995 [12] using ion traps as the physical system to perform computations. In this implementation, the use of lasers are needed to ionize atoms which are trapped in electric potentials. A more detailed explanation for set ups is presented in the next section of this manuscript.

4 DESIGN OF A QUANTUM COMPUTER

In this section we are going to explore more about the architectures and the designs of quantum computers and discuss how these hardware devices can be realized in a physical set up. It is important to mention that the following architectures require the use of classical computers to control the system because it is how the research has been directed to adopt and combine the hardware with some of the algorithms previously mentioned. After the measurement, the output that is produced by a Quantum computer (QC) is basically classical information which is later fed back to the classical computer for further processing.

To beging this section let's first point out some important pointsocurring in quantum hardware:

- **Universality**: First is to identify if the hardware platform for the quantum computer is a Turing-complete, or universal. If the device is a non-universal annealer, it is possible to test the DiVincenzo criteria previously described. Because DiVincenzo calls for the qubits to be individually addressable in a quantum computer, in the case of a two-level system comprised of an ensemble of atoms where the qubits are not individually addressable, this system would fail the QC test.

- **Fidelity**: is a measure of the ability for a qubit to remain in coherence through a computation.

- **Scalability**: The ability to scale the architecture of the QC to 10^6 qubits and beyond to achieve a fault-tolerant platform in that set up.

- **Qubits**: Considering the above conditions, design an architecture to mantaing the coherence of a large number of qubits.

- **Circuit depth**: How many operations can be implemented before the coherence breaks down.

- **Logical Connectivity**: Mantaining logical operations after implementing two-qubit gates on any pair of qubits.

- **Cloud access**: Make the hardware easily available in the cloud.

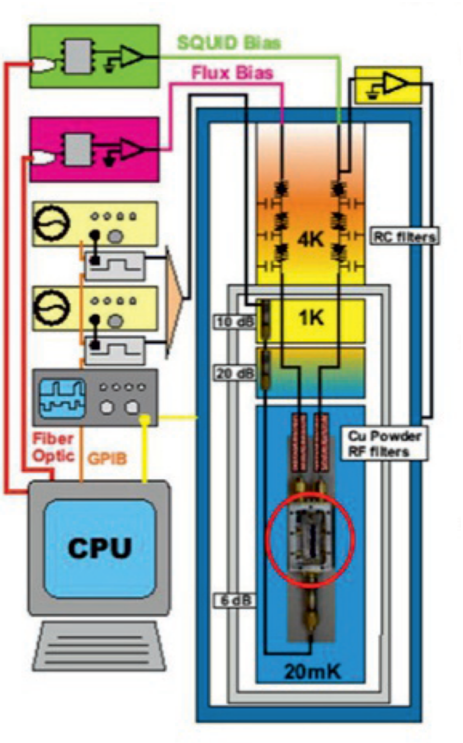

Figure 2: CPU controlling a superconducting QC [14]

With the above criteria, several architectures for a quantum computer have been explored over the years. Approaches such as Superconducting qubits, Trapped ions (the two leading approaches so far), Topological QC, Spin qubits, Photonics, Neural Atom are briefly described in the following subsections.

4.1 Trapped Ion

The trapped-ion approach uses ions (atoms electrically charged) as particles to be manipulated with lasers. Ytterbium atoms (more commonly used) are ionized with lasers and trapped in electric potentials to form a line of qubits (Figure 3). An additional laser is then used to tell the ions what operation to make. When the ions are exposed to the laser they get excited releasing photons. The qubit then is the state of ions emiting photonsand the number of ions released. An external system (a classical computer like in Figure 2) collects the photons and interpret the solution of an specific problem.

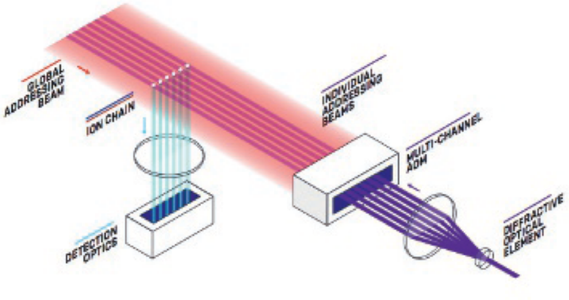

Figure 3: Diagram of a Trapped ion [15]

People like Cirac and Zoller worked in thi realm. Also Chris Monroe from University of Maryland, College Park and Jungsang Kim of Duke University have been active in this advances as well. Other groups include those at NIST [16], Oxford [17], Innsbruck [18], MIT [19] and ETH [20].

4.2 Superconducting Qubits

This architecture is based on the premise that the state of the qubit can be represented by particular electric circuits. The core of the design is that the electric circuit is made from a VCooper pair with a Josephson junction [21]. Such qubits can be manipulated with electrical input in the form of microwaves. By sending specific pulses of microwave frequencies for controlled amounts of of time into the physical qubit, the user can apply the range of unitary operators. The entire apparatus must be cooled below 10mK to operate. The system is also shielded from magnetic fields and other factors that could cause decoherence (Figure 2)

Several groups around the world are working on superconducting qubit quantum computers. Groups such as: Google, IBM, Rigetti, QCI and others.

One can compare the two architectures described above and in can tell the advantages and disadvantages of each case. For instance, Trapped Ion approach is easily manipulated, the quibits last longer time but the more ions on the trap, the more difficult is to control the system. It is why some reserch groups have creted smaller traps connected to each other by photons. On the other hand, Superconducting qubits make the operation faster that the ion traps and aslo, are easily scalable with the number of circuits yet, they are very fragile an live less time.

4.3 Photonics

Photonics can also be used to construct a gate-based quantum computer. Linear Optics Quantum Computing (LOQC) uses linear optical devices (such as mirrors, beam splitters and phase shifters) to process quantum information. The advantage of these elements is that they manating the coherence of input light and therefore apply a unitary transformation on a finite number of qubits. However, photons do not interact with each other in a vacuum. They can only interact indirectly via another medium.

Photonic chips can take advantage of the entire silicon-based infrastructure to miniaturize LOQC and reduce the cost. There are some researchers from the University of Bristol, as well as with researchers from China's National University of Defense Technology, have demonstrated a photonic quantum processor on a silicon photonics chip. The processor generates two photonic qubits on which it performs arbitrary two-qubit unitary operations, including arbitrary entangling operations [22].

4.3.1 Semiconductor Quantum transistor

There are some other researchers at the Joint Quantum Institute and the University of Maryland that have created the first single-photon switch and transistor enabled by solid-state quantum memory using a semiconductor chip [23]. Such device allows one photon to switch other photons, and therefore, produce strong and controlled photon-photon interactions. It consists of a spin qubit strongly coupled to a nanophotonic cavity (an idea first proposed by Duan and Kimble [24]). By using this solid-state transistor, they should be able to apply quantum gates to photons.

4.3.2 Topological photonic chip

This architecture is a promising option for a scalable QC because it doesn't require strong magnetic fields and feature intrinsically high-coherence for the qubits, room temperature and easy operation are some of the other advantages for this approach.

4.4 Topological QC

This topological approach uses the properties of anyons which are a 2-dimensional quasiparticle which is neither a boson (like photons) nor a fermion (like protons and electrons). By braiding the pathways of an anyion in 4D spacetime, it is theoretically possible to create a

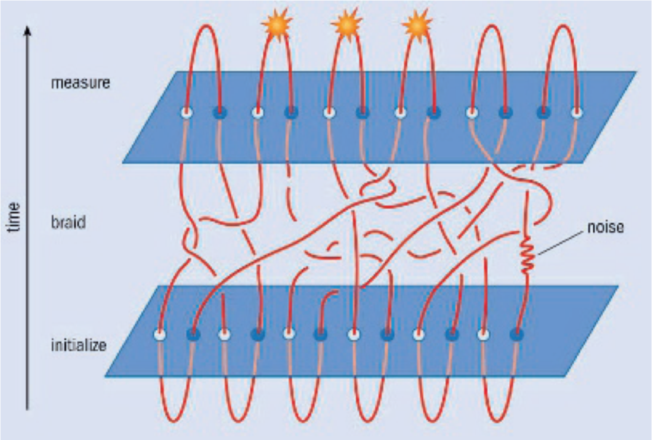

Figure 4: Anyons on a topological computer [25]

system difficult to decoher. Therefore, small perturbations to the system doesn't change the topology mantainig the coherence in the system of qubits (Figure 4).

Some other approaches for creating a QC involve the Neural Atom approach and some silicon-based spin-quibit technology commonly known as Spin Quibits. The latter is an alternative to not stop using the siliscon-based technologies to create qubits. As we have discussed researchers are exploring a wide range of architectures in the search for a faul-tolerant, scaled universal quantum computer but up to this day, understanding the problems innherent to these architectures is still an issue.

5 APPLICATIONS AND QUANTUM SUPREMACY

Up to this point, we have discussed why is QC important and relevant for the current technological updates, some key research and advances regarding the field of quantum computing and quantum information and how physicist and engineers are working in collaboration to develop algorithms and hardware; makes quantum computing possible in the coming decades. So, with all of this, what can we actually work with a Quantum computer? In other words, what are some of the applications that classical computers cannot perform due to the impossibility or the time-consuming processing?

In order to answer such questions, it is convenient to think for a moment within the realm of science in general. For instance, in chemistry, it exists a bunch of different complex processes that involve large number of atoms. Such collections of matter behave in a very complex way due to the amount of interactions that the particles have in large structures (such as proteins). Quantum simulations in chemistry could help researchers to develop new material, novel medical compounds and also have a better understanding of the fundamental behavior al small scales. IBM for example, has recently simulated the molecule beryllium hydride (BeH_2) on a seven-qubit quantum processor. This is a relatively small molecule with just three atoms and although the simulation doesn't use the approximations that are used in the classical computational approach, IBM's processor uses just a few qubits, making it possible to simulate the quantum processor using a classical computer.

In mathematics, it is possible to have a better patter recognition using probabilistic inference because a much larger distribution (which is one of the reasons to demonstrate a concept known as Quantum Supremacy). It can speed up the process of matrix inversion that has application in the industry such as computing electromagnetic patterns to design an antenna. Different optimization processes including transportation, online bidding strategies can be updated. New applications to the security data in financial transactions and interesting examples such as the replacement of the cryptography tools with more advanced protocols to avoid hacking.

Regarding the potential application by the private sector, nowadays companies like Microsoft, IBM, Google, D-Wave Systems, etc., have been financing research to reach the Quantum Supremacy. Such term was first coined by Preskill in 2012 and it refers to a computational task that can be efficiently performed on a quantum computer beyond the capabilities of what a classical supercomputer can efficiently implement [26]. In other words, to demonstrate the supremacy the algorithm to test it just need to have the ability to run more efficiently on a quantum processor than with a classical computer.

IBM is one of the most relevant companies that are currently working with superconducting qubits in its quantum computers. Back in 2016, IBM introduced a five-qubit processor that they have made available to everyone for free on the cloud so the common user can create their own quantum circuit with five qubits at most and run it on this computer. IBM's aim is to introduce quantum computing to a wide audience—circuits for a more dense coding. At the end of 2017, IBM connected a twenty-qubit computer to the cloud. This time it is not for education, but it is a commercial venture where companies can buy access.

Google is also working on its quantum computer and also uses superconducting qubits. This popular company is expected to announce in the near future that it has a computer that uses 72 qubits. Notice that the fewer qubits we have the better we can simulate them with classical computers. Google is expected to announce that it has reached or exceeded this number, giving them the right to claim quantum supremacy—the first time an algorithm has been run on a quantum computer that is impossible to run, or simulate, on a classical computer. IBM, however, is not giving up without a fight. Its team, using some innovative ideas, has recently found a way to simulate a 56-qubit system classically, increasing the lower bound on the number of qubits needed for quantum supremacy.

In late October 2019, Google anounced that the gap for reaching Quantum Supremacy has been reduced thanks to the $Sycamore\ Processor$ which is a parallel processor structure of 2^{53} states. Here, they activated 53 qubits that needed to detect certain structures in a random nmber series. The Sycamore processor solved the problem in 3:20 min. In comparison, the supercomputer IBM sumit would have taken 10,000 years to do so. However, IBM reponded that Google's statement was not very reliable because with a simple potence storage addition, the supercomputer would have solved it in 2.5 days. But despite all that, one thing that is notizable is that the investigation and dedication to the quantum information and quantum computing efforts for create a quantum machine is remarkable.

5.1 Quantum Error Correction

While today's quantum computers do not yet have sufficient qubits to support full quantum error correction (QEC), there is a growing body of research on QEC with implications for both QC and beyond.

Error correction schemes have also emerged from other branches of physics (in particular high energy physics); several researchers have been investigating QEC approaches that derive from the duality framework of Anti-de Sitter/Conformal Field Theory (AdS/CFT) [28]. QEC remains an active area of research and is critical in the scaling quantum computing hardware devices.

The AdS/CFT correspondence gives us an initial mapping between general relativity and quantum mechanics. As a matter of fact, is a dictionary that allows us to connect Quantum field theories with dimension d to theories with Gravity of dimension $d+1$. Leonard Susskind, Juan Maldacena, Edward Witten and many other researchers have speculated on the use of quantum computers to explore this duality [29]. This is because the concepts of quantum information are explored as a tool to understand better quantum entanglement and complexity theory which could lead to a better understanding of the universe and perhaps one of Einstein's dream of a Unified Field Theory.

6 FINAL REMARKS

Over the years fast pace of development in quantum computing has been done, both in hardware and software and with the efforts of so many reaserch Institutes and private companies it is expected to achieve more impact on that field. It is just matter of time to see quantum computers solving day by day issues that classical computers face today. Although we are still decades from harnessing the full potential of quantum computers, and perhaps some years from even doing anything usefull at all, quantum computing is edging even closer to those goals.

The quest of quantum implementation in computers, immediate leads to think that whoever wins the *race* for harnessing the power of quantum computing will have a notorious advantages over the ones that do not posses it. To exemplify this one can think of breaking cryptographic codes. If scalable quantum computer are avialable some day one could ask about What could happen if someone with a quantum computer wants to decipher private messages? Because companies are very involved in the creation of Quantum computers, should we expect them to create a database with the information from the users without the consent that thir information could be hacked? All those quastions are valid to ask due to the possible applications that Quantum computing are opening in the search of substituing the silicon-based technology for a more fundamental approach of computing. Problems such as identity robbery and the filtration of valuable personal information are very delicate and need to be taken into account when discussing quantum computing because a device that works in this way can out run a standard computer much faster. And although, in the present days nothing as been announced regarding the personal use of a quantum computer, it stands no reason that the quantum implementation will be exent of the problems that computers have nowadays.

Up to this day, all that we can say is that the race for quantum supremacy is starting to look promising, but it's important to remark that this is only the beginning phase. In the future (probabliy years from now or even decades) complex ethical debates will invade the topic of quantum computing.

References

[1] M. Born. Zur Quantenmechanik der Stoßvorgänge. Z. Phys., 37(12):863–867, 1926.

[2] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev., 47:777–780, May 1935.

[3] R. Landauer. Irreversibility and heat generation in the computing process. IBM Journal of Research and Development, 5(3):183–191, July 1961.

[4] R. P. Feynman. Feynman Lectures on Computation. CRC Press, 2000.

[5] A. Frisk Kockum. Quantum optics with artificial atoms. Chalmers University of Technology, 2014.

[6] 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, 22(5):563–591, May 1980.

[7] R. P. Feynman. Simulating physics with computers. International Journal of Theoretical Physics, 21(6):467–488, Jun 1982.

[8] D. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 400(1818):97–117, 1985.

[9] E. Bernstein and U. Vazirani. Proceedings of the 25th annual ACM symposium on the theory of computing. ACM, New York, 11, 1993.

[10] Y. Nakamura, Y. A. Pashkin, and J. Tsai. Coherent control of macroscopic quantum states in a single- Cooper-pair box. Nature, 398(6730):786, 1999. arXiv: cond-mat/9904003.

[11] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Rabi oscillations in a Josephson-junction charge two-level system. Phys. Rev. Lett., 87:246601, Nov 2001.

[12] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. Phys. Rev. Lett., 74:4091–4094, May 1995.

[13] D. P. DiVincenzo. Topics in quantum computers. arXiv preprint cond-mat/9612126, 1996.

[14] D. P. Pappas, J. S. Kline, F. da Silva, and D. Wisbey. Coherence in superconducting materials for quantum computing.
`https://slideplayer.com/slide/7770332/`

[15] K. Wright, K. Beck, S. Debnath, J. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. Pisenti, M. Chmielewski, C. Collins, et al. Benchmarking an 11-qubit quantum computer. arXiv preprint arXiv:1903.08181, 2019.

[16] J. G. Bohnet, B. C. Sawyer, J. W. Britton, M. L. Wall, A. M. Rey, M. Foss-Feig, and J. J. Bollinger. Quantum spin dynamics and entanglement generation with hundreds of trapped ions. Science, 352(6291):1297–1301, 2016.

[17] D. Lucas, C. Donald, J. P. Home, M. McDonnell, A. Ramos, D. Stacey, J.-P. Stacey, A. Steane, and S. Webster. Oxford ion-trap quantum computing project. Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 361(1808):1401–1408, 2003.

[18] N. Friis, O. Marty, C. Maier, C. Hempel, M. Holzäpfel, P. Jurcevic, M. B. Plenio, M. Huber, C. Roos, R. Blatt, et al. Observation of entangled states of a fully controlled 20-qubit system. Physical Review X, 8(2):021012, 2018.

[19] D. R. Leibrandt, J. Labaziewicz, V. Vuletic, and I. L. Chuang. Cavity sideband cooling of a single trapped ion. Physical Review Letters, 103(10):103001, 2009.

[20] C. Flühmann, T.L. Nguyen, M. Marinelli, V. Negnevitsky, K. Mehta, and J. Home. encoding a quibit in a trapped-ion mechanical oscillator. Nature, 566(7745):513, 2019

[21] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, and M. Devoret. Quantum coherence with a single cooper pair. Physica Scripta, 1998(T76):165, 1998.

[22] X. Qiang, X. Zhou, J. Wang, C. M. Wilkes, T. Loke, S. O'Gara, L. Kling, G. D. Marshall, R. Santagati, T. C. Ralph, et al. Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. Nature Photonics, 12(9):534, 2018.

[23] S. Sun, H. Kim, Z. Luo, G. S. Solomon, and E.Waks. A single-photon switch and transistor enabled by a solid-state quantum memory. arXiv preprint arXiv:1805.01964, 2018.

[24] L.M. Duan and H. Kimble. Scalable photonic quantum computation through cavity-assisted interactions. Physical Review Letters, 92(12):127902, 2004.

[25] S. Simon. Quantum computing...with a twist. Physics World, Sep 2010. https://physicsworld.com/a/quantum-computingwith-a-twist/.

[26] J. Preskill. Quantum computing and the entanglement frontier. arXiv preprint arXiv:1203.5813, 2012.

[27] S. Aaronson and A. Arkhipov. The computational complexity of linear optics. In Proceedings of the forty-third annual ACM symposium on Theory of computing, pages 333–342. ACM, 2011.

[28] A. Almheiri, X. Dong, and D. Harlow. Bulk locality and quantum error correction in ads/cft. Journal of High Energy Physics, 2015(4):163, 2015.

[29] L. Susskind. Dear qubitzers, GR=QM. arXiv preprint arXiv:1708.03040, 2017.

[30] E. Rieffel and W. Polak. An Introduction to Quantum Computing for Non-Physicist. ArXiv: quantph/ 9809016, 1998.

[31] M. Nielsen and I. Chuang. Quantum Computing and Quantum Information. CUP, 2011.

[32] P. Kaye et al. An introduction to Quantum Computing. Oxford University Press, 2007.

[33] V. Vedral. Introduction to Quantum Information Science. Oxford Univerity Press, 2006.

[34] F. Jazaeria, et al. A Review on Quantum Computing: Qubits, Cryogenic Electronics and Cryogenic MOSFET Physics. arXiv preprint arXiv:1908.02656, 2019.

[35] S. Resch and U. Karpuzcu. Quantum Computing: An Overview Across the system stack. arXiv preprint arXiv: 1905.07240, 2019.

[36] A. Steane. Quantum Computing. arXiv preprnt arXiv: quantph/9708022v2, 1997.

[37] M. Martonosi and M. Roetteler. Next Steps in Quantum Computing: Computer Science's Role. arXiv preprint, arXiv: 1903.10541, 2019.

[38] R. Wolf. Quantum Computing: Lecture Notes. arXiv preprint, arXiv: 1907.09415, 2019.

[39] J. Ossorio-Castillo and J. Tomero. Quantum Computing fom a mathematical perspective: a description of the quantum circuit model. arXiv preprint, arXiv: 1810.08277, 2018.

[40] Microsoft Quantum Team. The Microsoft approach to Quantum Computing. 2018. https://cloudblogs.microsoft.com/quantum/2018/06/06/the-microsoftapproach-to-quantumcomputing/

[41] D. Harlow.
https://danielsharlow.wordpress.com/ethics/

[42] IBM Q. Quantum Starts Here. (2019).
https://www.ibm.com/quantum-computing/

[43] Intel. Reinventing Data Processing wih Quantum Computing.
https://www.intel.com/content/www/us/en/research/quantumcomputing.html

[44] AI Podcast Clips. Leonard Susskind. The Power of Quantum Computers (28/sep/2019).
https://www.youtube.com/watch?v=3jNSlGHCOO0

[45] AI Podcast Clips. Leonard Susskind. The Power of Quantum Computers (26/sep/2019).
https://www.youtube.com/watch?v=s78hvV3QLUE

[46] R. Feynman. Computers Obeying Quantum Mechanical Laws. Summary file of the talk. Website:
https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-02-499-02