State of the art of quantum computing models and physical implementations

Clara Grimault, Jean-Adrien Ducastaing,
Ethan Rimo, Florian Gabille, Paul-Emile Morgades
Lotus Noir Quantum Computing Research Group - GITM Specialization
EPITA - Graduate School for Computer Science and Advanced Technologies

***Abstract*— This is a technical review of the current state of the quantum computing field in general as well as it's different models and physical implementations. While its meant to be as self-contained as possible and features a quick and non-exhaustive refresher, the understanding of this document requires the *GITM Quantum Computing 10x* course or basic understanding of quantum mechanics and computing. As an effort to be the most self-contained as possible and provide a wide review with only the basic theoretical requirements, some section will be less detailed than others.**
This review will be segmented as follows: -

1) **Quick refresher of general quantum computing basic mathematical model.**
2) **Current state of quantum computing in general.**
3) **Description and comparison of main models and trends in quantum computing.**
4) **Review of the current proposed and applied physical implementations of such models**

I. Quantum Computing Mathematical Model Refresher[1][2][3][4]

A. Basic Quantum Theory

We can introduce the basics by following a simplistic scenario in which we assume we can describe every possible states of a particle as a finite set of n vectors $|x_i\rangle$ such as:

$$|x_0\rangle \rightarrow \begin{bmatrix}1 & 0 & ... & 0\end{bmatrix}^T$$

$$|x_1\rangle \rightarrow \begin{bmatrix}0 & 1 & ... & 0\end{bmatrix}^T$$

$$...$$

$$|x_{n-1}\rangle \rightarrow \begin{bmatrix}0 & 0 & ... & 1\end{bmatrix}^T$$

Since the current system is quantum and does not obeys to the rules which would apply to a classical system, we need to define it by all possible combinations of states as possible states. Thus let $|\psi\rangle$ be an arbitrary state that can be described as a linear combinations of all the above states, for the suitable known complex weights $(c_0, c_1, ..., c_{n-1}) \in C^n$ can be written as:

$$|\psi\rangle = c_0 |x_0\rangle + ... + c_{n-1} |x_{n-1}\rangle$$

We define the **basis** of the system as all the possible outcome states x_i thus we can represent $|\psi\rangle$ by just knowing the coefficients c_i.
The current state $|\psi\rangle$ is said to be in **superposition** of all the basic states $|x_i\rangle$, which means it lies on all states simultaneously, however when we observe it, the state will collapse to one of the basic states with a probability of $\frac{|c_i|^2}{||\psi\rangle|^2}$, thus the modulus squares of the complex numbers c_i plays the role of the probabilities of the state being collapsed to that basic state.

The **bra-ket** notation is the way to describe vectors and inner products (dot products) of vectors in quantum mechanics. Let $\langle\phi|$ and $|\psi\rangle$ be two vectors in C^n, the difference between those vectors is the orientation: $|\psi\rangle$ is called the *ket* and represents a column vector; $\langle\phi|$ is called the *bra* and represents a Hermitian conjugate of a ket ($\langle X| = \overline{|X\rangle}^T = |X\rangle^\dagger$), and thus it is a row vector.

The standard notation for inner product in the bra-ket notation is:

$$\langle\phi|\psi\rangle \equiv (\langle\phi|) \cdot (|\psi\rangle)$$

$$= \begin{bmatrix}\overline{\phi_1} & \overline{\phi_2} & ... & \overline{\phi_n}\end{bmatrix} \cdot \begin{bmatrix}\psi_1 \\ \psi_2 \\ ... \\ \psi_3\end{bmatrix}$$

The inner product satisfies the following properties:

- Conjugate Symmetry: $\langle X|Y\rangle = \overline{\langle Y|X\rangle}$
- Positive Definiteness: $\langle X|X\rangle \geq 0$
- Linearity: $\langle X|\alpha \cdot Y + \beta \cdot Z\rangle = \alpha \langle X|Y\rangle + \beta \langle X|Z\rangle$

Since the *"bra-ket vectors"* are defined in C^n and the inner product satisfies the above properties, we can show that those vectors are defined in a **Hilbert space**.

Similarly, the standard notation for the outer product is:

$$|\phi\rangle \langle\psi| \in C^{n\times n}$$

Some other properties of *"bra-ket vectors"* are:

- $\langle\phi|^\dagger = |\phi\rangle$ and $|\phi\rangle^\dagger = \langle\phi|$
- Let $|\psi\rangle = c_0 |x_0\rangle + c_1 |x_1\rangle + ... + c_{n-1} |x_{n-1}\rangle$ and $|\psi'\rangle = c'_0 |x_0\rangle + c'_1 |x_1\rangle + ... + c'_{n-1} |x_{n-1}\rangle$ then $|\psi\rangle + |\psi'\rangle = (c_0 + c'_0) |x_0\rangle + (c_1 + c'_1) |x_1\rangle + ... + (c_{n-1} + c'_{n-1}) |x_{n-1}\rangle$
- Bras and kets can be multiplied by scalars.

Let $|b_0\rangle, ..., |b_{n-1}\rangle$ a collections of kets that form a basis in C^n. Then, any ket in C^n can be written as a linear combination of these basis vectors:

$$|\psi\rangle = c_0 |b_0\rangle + ... + c_{n-1} |b_{n-1}\rangle$$

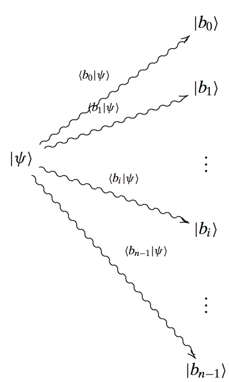

Fig. 1. Transition from a state in superposition to its collapsed outcome is denoted by the inner product between the superposed state and the outcome.

The state after measurement/observation ends in any of the basis $|b_i\rangle$, where the probability is given by $|c_i|^2$. The transition from $|\psi\rangle$ to $|b_i\rangle$ is denoted by the inner product $\langle b_i|\psi\rangle$ which is called a **transition amplitude**.

We call "observables" the physical quantities that can be observed in each state of the state space. Each observable may be thought of as a specific question we pose to the system: assuming it is in the state $|\psi\rangle$, what values/quantities can we possibly observe?
An **observable** corresponds to an linear operator: given a state $|\psi\rangle \in C^n$, let us define an observable $\Omega \in C^n$. The action of the observable is denoted as $\Omega |\psi\rangle$ and it's by itself a state.
In quantum mechanics, each observable-linear operator is hermitian, which means that it has real eigenvalues. Then, the eigenvalues of an observable are the only possible values the observable can take, as a result of measuring it on a given state.
For a k-state quantum system, observables correspond to $k \times k$ hermitian matrices.
If we consider the state:

$$|\psi\rangle = c_0 |b_0\rangle + ... + c_{n-1} |b_{n-1}\rangle$$

Then the result of measurement $\Omega |\psi\rangle$ must be some $\lambda_i \in R$ with a probability $|c_i|^2$. Moreover, the after this measurement the state of the system is collapsed to $|\psi_i\rangle$.

In other words, an observable is an operator that corresponds to a physical quantity, such as energy, spin, or position, that can be measured; think of a measuring device with a pointer from which you can read off a real number which is the outcome of the measurement.

Any transition from a quantum state $|\psi_t\rangle$ to a $|\psi_{t+1}\rangle = U |\psi_t\rangle$ state must be done via a **unitary operator** which is represented as a matrix U and follows the following properties:

- $UU^\dagger = U^\dagger U$ with $U^\dagger = \overline{U}^T$
- $\|U \cdot |x\rangle\| = \||x\rangle\|$ (preservation of norm)
- $|\langle U \cdot |x\rangle | U \cdot |y\rangle\rangle| = |\langle x|y\rangle|$ (preservation of inner product)

The differences between observables and generic unitary transformations is that the latter satisfy:

- the product of two unitary matrices is always unitary (in any order);
- the inverse of a unitary matrix is unitary.

B. Entanglement

Let us consider a multi-particle system composed of two particles which possess respectively the superposed states $X \equiv x_0, x_1, ..., x_{n-1}$ and $Y \equiv y_0, y_1, ..., y_{m-1}$, we can create the assembly of states by using the **tensor product** $X \otimes Y$, where the possible states are:

$$|x_0\rangle \otimes |y_0\rangle$$

$$|x_0\rangle \otimes |y_1\rangle$$

$$...$$

$$|x_1\rangle \otimes |y_0\rangle$$

$$...$$

$$|x_{n-1}\rangle \otimes |y_{m-1}\rangle$$

Here, $|x_i\rangle \otimes |y_j\rangle$ means that the first particle is in state i of X and the second particle is in the state j of Y

Using all possible combinations, we can write down the state of two particles as a superposition of basic states such as:

$$|\psi\rangle = c_{0,0} \cdot |x_0\rangle \otimes |y_0\rangle + ... + c_{n-1,m-1} \cdot |x_{n-1}\rangle \otimes |y_{m-1}\rangle$$

With the probability of the system being in a state $|x_i\rangle \otimes |y_j\rangle$ equals to:

$$P(|x_i\rangle \otimes |y_j\rangle) = \frac{|c_{i,j}|^2}{\sum_{x \in [0,n-1], y \in [0,m-1]} |c_{x,y}|^2}$$

However, in the case of quantum systems, we cannot always describe the overall system by looking into the constituents. For example, let us assume the simple case above where $n = m = 2$, and let us assume that the current state $|\psi\rangle$ satisfies:

$$|\psi\rangle = |x_0\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$$

$$= 1 \cdot |x_0\rangle \otimes |y_0\rangle + 0 \cdot |x_0\rangle \otimes |y_1\rangle +$$

$$0 \cdot |x_1\rangle \otimes |y_0\rangle + 1 \cdot |x_1\rangle \otimes |y_1\rangle$$

Let us see whether we can describe the above state as the tensor product of the basic states of single particles. The state described by using only the first particle can be expressed as:

$$c_0 \cdot |x_0\rangle + c_1 \cdot |x_1\rangle$$

and the state using only the second particle can be described as:

$$c'_0 \cdot |y_0\rangle + c'_1 \cdot |y_1\rangle$$

Thus if we try to models the whole system states by assembling the simpler systems, we compute the tensor product of their states, In particular we have:

$$(c_0 \cdot |x_0\rangle + c_1 \cdot |x_1\rangle) \otimes (c'_0 \cdot |y_0\rangle + c'_1 \cdot |y_1\rangle) =$$

$$c_0 c'_0 \cdot |x_0\rangle \otimes |y_0\rangle + c_0 c'_1 \cdot |x_0\rangle \otimes |y_1\rangle +$$

$$c_1 c'_0 \cdot |x_1\rangle \otimes |y_0\rangle + c_1 c'_1 \cdot |x_1\rangle \otimes |y_1\rangle$$

We need to choose the coefficients to create $|\psi\rangle$. However this means that $c_0 c'_0 = c_1 c'_1 = 1$ and $c_0 c'_1 = c_1 x'_0 = 0$ which is impossible. Thus those two equations have no solutions: we cannot use the basic states and the tensor product to generate the state. In this case, we say that the two particles are **entangled**.

In practice that means that if we measure the first particle in state x_0, we can use this information to infer the state of the second particle. Indeed, we can see that the component $|x_0\rangle \otimes |y_1\rangle$ has coefficient 0 in the expression of the state of the two particles. This means that, if we found the first particle in x_0, we will find the second particle in the state y_0. It is possible to infer the state of the individuals particles even if they are light years away.

Thus, if we can infer information of some particle by looking some others, we say that the particles are entangled. If this is not the case, then the particles are **separable**.

C. Quantum Information

In the macroscopic word, we know that:

- electricity either passes or not through a circuit
- a proposition is true or false

The above can be easily described through a bit: a bit represent an way to say that we are in a particular state among two states.

$$|state\rangle = \begin{bmatrix} state = 0 \\ state = 1 \end{bmatrix}$$

Observe that in our macroscopic world, the state cannot be in both situations. More rigorously, let us represent the state 0 as:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and the state 1 as:

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

We can see that these two representations are orthogonal: we cannot be in a situation where a bit is in a superposition of the state $|0\rangle$ and the state $|1\rangle$.

A quantum bit (**qubit**) is a generalization of the classical bit. Using the notion above, a quantum bit can be described as:

$$|0\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

where $|c_0|^2 + |c_1|^2 = 1$. But note that while $|c_i|^2$ is a probability, when we measure the quantum bit, it "**collapses**" to a classical bit. We can visualize this as:

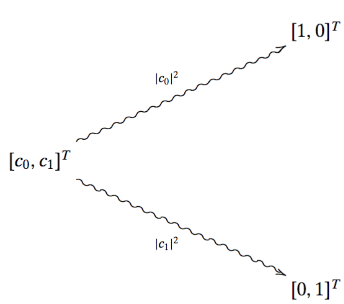

Fig. 2. Upon measurement, a qubit collapse into one of it's possible outcome bit (state).

Before measuring it, any qubit can be written as a linear combination of classical bits:

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$$

We define multi-particles (qubits) states, which are called **quantum registers** such as:

$$|01...1\rangle = |0\rangle \otimes |1\rangle \otimes ... \otimes |1\rangle$$

Therefore, with n qubits, we can represents 2^n bits. Which is one of the main motivations of quantum computing.

II. Motivations, Current State and Usages of Quantum Computing[3][5][6]

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space.

In the early 1980s, **Richard Feynman** proposed that a quantum computer would be an effective tool with which to solve problems in physics and chemistry, given that it is exponentially costly to simulate large quantum systems with classical computers[7].

The major technical and theoretical challenges to be resolved are in particular:

- can a quantum system be engineered to perform a computation in a large enough computational (Hilbert) space and with a **low enough error rate** to provide a quantum speedup?
- can we formulate a problem that is hard for a classical computer but easy for a quantum computer?

The first question could be potentially answered by the recent *Google* breakthrough, which has arguably demonstrated the achievement of **quantum supremacy**[5] on cross-entropy benchmarking[14]. It is still unknown if such feat could be generalized in the future.

We can try to pinpoint the applications of quantum computing from a complexity theoric point of view. As refresher, let us define the most common computational complexity classes:

- P: Class of problems which can be solved in polynomial time.
- NP: Class of computational decision problems for which a given solution can be verified as a solution in polynomial time.
- NP-hard: Class of problems which are at least as hard as the hardest problems in NP. Problems that are NP-hard do not have to be elements of NP; indeed, they may not even be decidable.

It is admitted that $P \subseteq NP$, however the assumption that $P \neq NP$ has not been proved yet and represents one of the most important unproved theorem in modern complexity theory.

In 1972, Stephen Cook proved that the intersection of the NP-hard and NP classes is not empty[11], this intersection is designated as NP-complete. NP-complete problems are in essence the hardest of the NP problems.

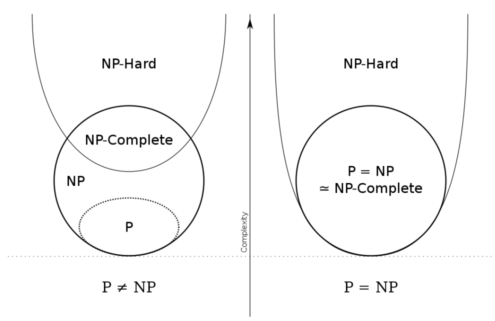

Fig. 3. Since it the equality $P = NP$ has not been proved or unproved, we need to represents the two alternatives to be rigorous.

If an efficient algorithm for a NP-complete problem were found, it could be adapted to solve all the other NP problems in **polynomial time** as well, thus implying that $NP = P$.

However, no such algorithm has been discovered yet and the widely-adopted assumption that $P \neq NP$ stands[10]. Thus the only hope to solve such problems in polynomial times, if it is possible, would be to rely on non-classical computing: quantum computing.

While there are some pointers that suggest that quantum computers could not offer more than a polynomial speedup to the NP-complete problems[9], [10], [12], such a speedup, assuming that it could not be improved further, would struggle against heuristic approaches but still could be of significant benefit for problems requiring exact solutions or for problems that can classically be solved in sub-exponential time.

The ultimate goal of quantum computing is quantum supremacy, which was recently described in [13] as follows:

Quantum supremacy is achieved when a formal computational task is performed with an existing quantum device which cannot be performed using any known algorithm running on an existing classical super-computer in a reasonable amount of time.

As we have quickly explained the motivations and the current general state of quantum computing, let us introduce some of the most anticipated potential quantum computing applications.

A. Factoring Problem

By the fundamental theorem of arithmetic, every positive integer n has a unique prime factorization such as:

$$n = pq$$

with p and q prime numbers. The practical importance of the factorization (which a NP problem but conjectured to be outside P) problems lies in it's usage in RSA algorithm in which n is the public key while p and q are part of the private key, an efficient factoring algorithm could allows to easily break such cryptography algorithms.

However, it seems that the achievement of quantum supremacy on such problem via **Shor's Algorithm**[8] is not foreseeable in the near future[9].

On a classical computer the complexity of the algorithm use for factorizing a number exponentially grows according to the number of bit used for representing the number. Therefore this task cannot be perform for large number. Nevertheless for a quantum computer it grows in a polynomial way. Therefore this task can be performed for an arbitrary large number.

B. Search in a Database[15]

A quantum mechanical algorithm that can query information relating to multiple items of the database containing N items, can search a database for a unique item satisfying a given condition, in a single query (a query is defined as any question to the database to which the database has to return a "yes" or "no" answer). A classical algorithm will be limited to the information theoretic bound of at least $\log_2 N$ queries, which it would achieve by using a binary search.

However the query is complicated as preparing the query and processing the results of the query take $\Omega(N \log N)$ steps.

The algorithm works by considering a quantum system composed of multiple subsystems; each subsystem has an N dimensional state space like the one used in the quantum search algorithm[16], each basis state of a subsystem corresponds to an item in the database.

It is shown that with a single quantum query, pertaining to information regarding all N items, the amplitude (and thus probability) in the state corresponding to the marked item(s) of each subsystem can be amplified by a small amount.

By choosing the number of subsystems to be appropriately large, this small difference in probabilities can be estimated by making a measurement to determine which item of the database each subsystem corresponds to the item pointed to by the most subsystems is the marked item.

C. Machine Learning[17]

A significant fraction of the field of machine learning deals with data analysis, classification, clustering, etc. Quantum information generalizes standard notions of data to include quantum states.

Machine learning concepts can be extended to the quantum domain, mostly focusing on specific aspects of supervised learning and learn ability of quantum systems but also on concepts underlying reinforcement learning.

However, machine learning is more than a sum of such specific-task-solving parts, and in this sense even radical quantum speed-ups in the solving of such tasks may result only in a limited improvement.

D. Quantum Physics Simulation[18]

Simulating a fully general quantum system on a classical computer is possible only for very small systems, because of the exponential scaling of the Hilbert space with the size of the quantum system.

Let us consider the classical memory required to store a quantum state $|\psi\rangle$ composed of n qubits. Considering that all the 2^n possible states x_i of $|\psi\rangle$ can be in superposition in different proportions, we can represent it as:

$$\sum_{i=0}^{2^n-1} c_i \, |x_i\rangle$$

To store this state in a classical computer, we need to store all the complex coefficients c_i, each of those coefficients requires two floating point numbers (real and imaginary parts). Using 32 bits (4 bytes) for each floating point number, a quantum state of $n = 27$ qubits would require 1 Gbyte of memory.

Since each additional qubit doubles the memory, 37 qubits would need a Terabyte of memory. Thus physics systems represented with a high number of qubits could only practically be simulated on quantum computers.

III. Review of Current Quantum Computing Models

There are more than one way to modelize quantum computation, in this document we will review the 4 more influential computing models at the current day.
Each of these models have their own perks and drawbacks and some are more pro-efficient in some specific field of applications than others.

A. *Quantum Gate Array[19]*

Also been known as Uncommitted Logic Arrays (ULAs) and semi-custom chips, a gate array is a type of ASIC (application-specific integrated circuit) chip that is partially finished with rows of unconnected transistors and resistors. Nowadays, it is rarely used.

Programmable quantum gate arrays are fixed circuits which take as input a quantum state specifying a quantum program and a data register, to which the unitary operator corresponding to the quantum program is applied. The initial state in such model can be described as:

$$|d\rangle \otimes |P\rangle$$

where $|d\rangle$ is a state of a m qubits data register and $|P\rangle$ is a state of the n qubits program register, the two registers are not entangled.

The processing of of this state by the programmable gate array is given by a unitary operator G such as:

$$|d\rangle \otimes |P\rangle \rightarrow G[|p\rangle \otimes |P\rangle]$$

Where the gate array is said to implement a unitary operator U acting on m qubits if a state $|P_U\rangle$ of the program register exists such that:

$$G[|d\rangle \otimes |P_U\rangle] = U\,|d\rangle \otimes |P'_U\rangle$$

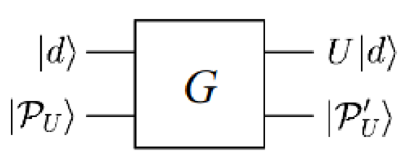

Fig. 4. Representation a such quantum gate array which implements the unitary operation U applied on $|d\rangle$ and determined by the quantum program P_U.

B. *One-Way Quantum Computation[20]*

One-Way quantum computation requires qubits to be initialized in a highly-entangled cluster state or graph state. From this point, the quantum computation proceeds by a sequence of single-qubit measurements with classical feed-forward of their outcomes, thus allowing universal quantum computation through single-qubit measurements alone. These operations are irreversible, thus preventing the measurement to take place simultaneously, forcing a sequential mode of operation.

Measurements on entangled states play a key role in many quantum information protocols, such as quantum teleportation and entanglement-based quantum key distribution. In these applications an entangled state is required, which must be generated beforehand. Then, during the protocol, measurements are made which convert the quantum correlations into, for example, a secret key.

This entangled state, can be considered a resource which is used in the protocol. The quantum algorithm is specified in the choice of bases for these measurements and the structure of the entanglement of the resource state.

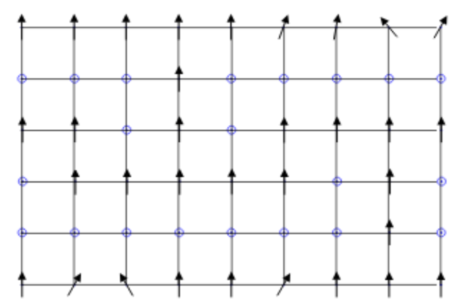

Fig. 5. One way quantum computation consists of single-qubit measurements in certain bases and in a certain order on an entangled resource state. Cluster states have a square lattice (”grid”) structure.

The name one-way reflects the resource nature of the graph state. The state can be used only once, and irreversible measurements drives the computation forward.

Cluster states are a sub-class of graph states. The extra flexibility in the entanglement structure of graph states means that they often require far fewer qubits to implement the same one-way quantum computation. However, there are a number of physical implementations, such as optical lattices, where the regular layout of cluster states means that they can be generated very efficiently.

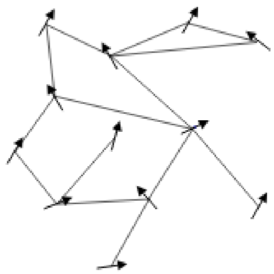

Fig. 6. Choosing a specific graph state instead of cluster state can reduce the number of qubits needed for a computation significantly.

C. Adiabatic Quantum Computation[21]

Instead of evolving computations by encoding qubits in a Hilbert space, AQC proceeds from an initial Hamiltonian (operator corresponding to the sum of all kinetic and potential energy of the particles in the system) whose ground state is easy to prepare, to a final Hamiltonian whose ground state encode the solution to the problem. The adiabatic theorem guarantees that the system will track the instantaneous ground state provided the Hamiltonian varies sufficiently slowly.

Adiabatic quantum computation will only offer a polynomial speedup over its classical counterpart as opposed to the exponential speed up offered by standard quantum computation.

To introduce the model more formally, it is necessary to define the notion of k-local Hamiltonian. A Hamiltonian is a Hermitian matrix acting on quantum states, this its dimensions are $2^n \times 2^n$ for a system of n qubits. A k-local Hamiltonian is a Hamiltonian which can be written as the sum of Hamiltonians, each of which act on k qubits at most instead of all n qubits.
Thus, Adiabatic Quantum Computation can be formally defined such as:

A k-local adiabatic quantum computation is specified by two k-local Hamiltonians H_0 and H_1 acting on n particles. The ground state of H_0 is unique, the output is a state whose l_2-norm is nearly equal (ϵ-close) to the l_2-norm of the ground state of H_1. Let $s(t) : [0, t_f] \rightarrow [0, 1]$ the *"schedule"* where t_f is be smallest time such that the final state of an adiabatic evolution generated by $H(S) = (1 - s)H_0 + sH_1$ for time t_f is ϵ-close in l_2-norm to the ground state of H_1.

This definition thus demonstrates that this model is very analog to an optimization problem, where H_1 represents a classical optimization problem to be minimized, multiple final ground states do not pose a problem as any of the final states represents a solution to the optimization problem.

D. Topological Quantum Computation[22]

A topological quantum computer makes computation by braiding quantum particle around them. The computation does not come from the state of particle, but from their positions in space.

Both the encoding and the processing are inherently resilient against errors due to their topological nature, thus promising to overcome one of the main obstacles for the realization of quantum computers.

Topological quantum computation is an approach to storing and manipulating quantum information that employs exotic quasiparticles, which are emergent phenomena occurring when a microscopically complicated system behaves as if it contained different interacting particles, called anyons.

Anyons are interesting on their own right in funda-mental physics, as they generalise the statistics of the commonly known bosons and fermions. Due to this exotic statistical behaviour, they exhibit non-trivial quantum evolutions that are described by topology, they are abstracted from local geometrical details.

When anyons are used to encode and process quantum information, this topological behaviour provides a much desired resilience against control errors and perturbations.

Unfortunately, the theoretically proposed states that support the necessary types of anyons are very fragile and thus experimentally challenging.

Thus, this computation model have never been successfully implemented yet.

IV. Review of Physical Implementations[23]

Many quantum computer physical have been proposed and, for some, applied over time. There are many metrics to benchmark them, such as:

- **Coherence Time** is a measure of typically how long quantum states that represent qubits remain coherent, which correspond to the ability of preserve the information carried by the qubit state against quantum noise. Longer times are preferable. This gives one more time to complete a quantum operation, allowing more operations (a deeper quantum circuit) to take place in a given algorithm. By the same token, error correction will have to be applied less frequently, creating a lower overhead.

- **Gate Latency** is how long it takes to perform a single quantum operation. A lower latency has a similar effect to longer coherence time. The shorter gate operations are, the more that can be performed before decoherence of the quantum state occurs. Latency is highly dependent on the physical technology but is also determined by the specific methods used to implement it. There is typically an optimal latency which introduces the least amount of noise.

- **Gate Fidelity** is how likely a gate will be performed without introducing error. It is why coherence time and gate latency are not linearly related. While lower gate latency allows more operations to occur within the typical coherence time, these gates introduce more opportunities for decoherence. Fidelity for quantum operations are substantially lower than in classical computing, often less than 99%.

These metrics will be displayed on all implementation described below if available from [23].

A. *Superconducting Quantum Computer[24]*

- Coherence Time (s): $7.0e^{-6}$-$9.5e^{-5}$
- 1-Qubit Gate Latency (s): $2.0e^{-8}$-$1.30e^{-7}$
- 1-Qubit Gate Fidelity (%): 98-99.92

This implementation works thanks to superconducting electronic circuit. It is the most chosen implementation. All the most recent and important quantum computing breakthroughs have been achieved with through this implementation[23].

The main advantage relies in the fact that it makes the quantum effects become macroscopic, thus making the measurement of the outcome of an operation easier.

One remarkable feature of superconducting qubits is that their energy-level spectra (wavelengths of light emitted from an element when it's electrons lose energy) are governed by circuit parameters and thus are configurable; they can be designed to exhibit atom-like energy spectra with desired properties.

Therefore, superconducting qubits are also often referred to as artificial atoms, offering a rich parameter space of possible qubit properties with predictable performance.

The main limitations of this implementation lies in the small number of qubits which each qubit can interact with and the very low experimental temperature parameters needed for the superconductors involved.

B. *Trapped Ion Quantum Computer[25]*

- Coherence Time (s): 0.2-0.5
- 1-Qubit Gate Latency (s): $1.6e^{-6}$-$2.0e^{-5}$
- 1-Qubit Gate Fidelity (%): 99.1-99.9999

Ions (or charged atomic particles) can be confined and suspended in free space using electromagnetic fields. Qubits are stored in stable electronic states of each ion, and quantum information can be transferred through the collective quantized motions of the ions in a shared trap. Lasers are applied to induce coupling between the qubit states.

The basic requirements for universal quantum computing have all been demonstrated with ions, and quantum algorithms using few-ion-qubit systems have been implemented.

However, despite the promise shown by trapped ions, there are still many challenges that must be addressed in order to realize a practically useful quantum computer. There is most importantly the problem of increasing the number of simultaneously trapped ions while maintaining the ability to control and measure them individually with high fidelity.

It is hard to find good ions that can be favorable for multiple quantum computing architectures. Most of ions need ultraviolet light to be manipulated, and this type of light is hard to work with. However, technology that deliver visible and infrared light already exist so we need ions that can be manipulated by these types of light.

C. Nuclear Magnetic Resonance Quantum Computers

- Coherence Time (s): 16.7
- 1-Qubit Gate Latency (s): $2.5e^{-4}$-$1.0e^{-3}$
- 1-Qubit Gate Fidelity (%): 98.74-99.60

Nuclear magnetic resonance is a method of physical observation in which nuclei in a strong constant magnetic field are perturbed by a weak oscillating magnetic field and respond by producing an electromagnetic signal with a frequency characteristic of the magnetic field at the nucleus.

Gershenfeld and Chuang[30] propose the use of a system of nuclear magnetic resonance of molecules in a room-temperature solution. They demonstrate that such a bulk spin-resonance system is capable in principle of doing quantum computation, and they discuss the generation of 6 to 10 quantum bits.

There exists two types of NMR base quantum computers:

- Liquid State NMR: Despite the fact of that NMR base quantum computers as been demonstrated that they can be created, a huge down side of using NMR is that the expected signal of an ideal quantum computer is 28 orders of magnitude smaller than the room temperature magnetization in a 100-spin system at room temperature. To catch this signal is really difficult.

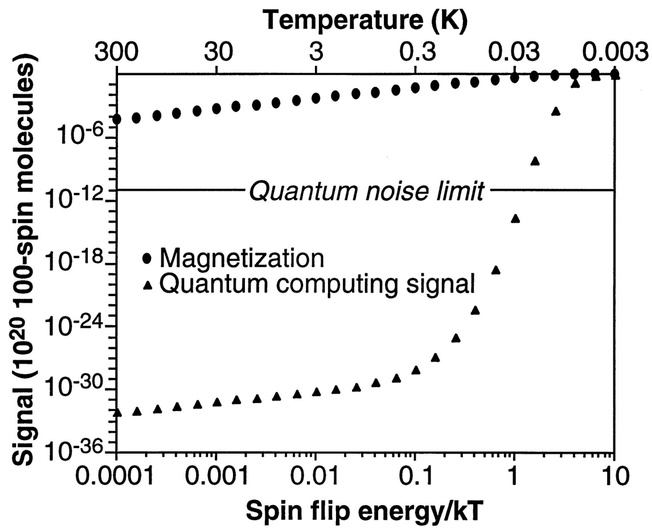

Fig. 7. LSNMR Quantum Signal Intensity

The ideal signal is small until T ¡ 0.01K, at which point the sample would surely not be a liquid solution.

- Solid State NRM: This implementation differs from LSNMR in that we have a solid state sample, for example a nitrogen vacancy diamond lattice rather than a liquid sample [32]. This has many advantages such as lack of molecular diffusion decoherence, lower temperatures can be achieved to the point of suppressing phonon decoherence and a greater variety of control operations that allow us to overcome one of the major problems of LSNMR that is initialisation. Moreover, as in a crystal structure we can localize precisely the qubits, we can measure each qubit individually, instead of having an ensemble measurement as in LSNMR.

D. Optical Lattices[26]

An optical lattice is formed by the interference of counter-propagating laser beams, creating a spatially periodic polarization pattern. The resulting periodic potential may trap neutral atoms via the Stark shift. Atoms are cooled and congregate in the locations of potential minima.

In a nutshell, optical lattices are crystals made of light which can be used to trap atoms at very low temperatures. When used in quantum computing, the qubit are implemented by the internal states of neutral trapped atoms.

Unlike the ultracold charged atoms trapped in electric fields (see the trapped ion quantum computer), the atoms trapped in different wells of an optical lattice hardly influence one another, so a million atoms can potentially be operated upon at once with this implementation.

But so far, about a million cesium atoms have been cooled in a two-dimensional optical lattice, but none of the logic operations have been performed on them.

E. Quantum Dot Computer[27]

- Coherence Time (s): $1.0e^{-6}$-$4.0e^{-4}$
- 1-Qubit Gate Latency (s): $1.0e^{-9}$-$2.0e^{-8}$
- 1-Qubit Gate Fidelity (%): 98.6-99.9

In this implementation, qubits are represented by the electron position in a doubles semiconductor quantum dot, containing one electron each and consisting each of two tunnel-connected parts.

Quantum dots are rare-earths-free and a lot less pollutant to produce or to recycle than usual batteries ans screens using mineral semi-conductors.

However, keeping quantum bits in the same physical state for a longer period of time is still a challenge.

F. Linear Optical Quantum Computer[34]

Linear optical quantum computing uses polarized photons as information carriers, mainly uses linear optical elements, to process quantum information, and uses photon detectors and quantum memories to detect and store quantum information.

The primary advantage of an optical approach to quantum computing is that it would allow quantum logic gates and quantum memory devices to be easily connected together using optical fibers or wave-guides in analogy with the wires of a conventional computer.

The main drawback to an optical approach has been the implementation of the quantum logic gates needed to perform calculations. Although several ingenious methods for producing nonlinear interactions at single-photon intensity levels have been considered, they are thought to be either too weak or accompanied by too much loss to be of use for practical quantum operators.

G. Rare-Earth-Metal-Ion-Doped Inorganic Crystal Based Quantum Computer

The electron dipole-dipole interaction between the ions that usually causes instantaneous spectral diffusion is used to generate the conditional phase shift. Due to their potential for long coherence times, dopant ions have long been considered promising candidates for scalable solid state quantum computing.[28]

Implementing high-fidelity quantum gate operations by means of the static dipole interaction, requires the participating ions to be strongly coupled, and the density of such strongly coupled registers in general scales poorly with register size. Moreover, the demonstration of two qubit operation has proven to be problematic, largely due to the difficulty of addressing closely spaced ions.[29]

H. Cavity Quantum Electrodynamics[35]

Cavity quantum electrodynamics (cavity QED) is the study of the interaction between light confined in a reflective cavity and atoms or other particles, under conditions where the quantum nature of light photons is significant. Photons bounce back and forth between two mirrors and an atom is send into the cavity.

The atom will be impacted by the numbers of photons in the cavity, and thus, we can determinate the quantity of photons inside the cavity without destroying them like others detectors usually do. [33] Using the numbers of photons in a cavity as the state of a qbits, this methods can be used to create quantum computers.

The two ways in which cavity QED techniques may be used to perform quantum computations are:

- Quantum information can be represented by photon states, with atoms trapped in cavities providing the non-linear interactions between photons, necessary for entanglement.
- Quantum information can be represented by atoms in different states,where photons are used to communicate between the different atoms/states.

Any realization of these approaches would at some point have to address the problem of precision control of population transfer, as a means to generate single photons. Such precision is a mandatory pre-requisite which is still not reached by current experimental standards.

V. Conclusion

Through this review we have exposed the very basic mathematical basis of quantum computing on which we built upon a general awareness of the current quantum computing state and field of applications and explored many papers treating a wide range of subjects.

As shown in the general quantum computing section, **the feasibility of general quantum supremacy is far from demonstrated** and it is still not known if quantum computing could in the future provide any major improvement of current computation capabilities.

We also exposed most quantum computing models and physical implementations, most of them have, however, not yet been demonstrated as practical due to current experimental challenges that have not been surpassed yet. But some of the showcased models/implementations are promising while significant **computational superiority through them not yet demonstrated**.

It is critical to note than most of the most notorious potential applications **relies in a exponential quantum computational speedup**, and as we shown through this review, it is not known if a quantum speedup, if possible, would be more than polynomial.

Due to the mostly **entry-level self-contained educational** aim of this review, some recent work have been ignored, preferring original publications of some concepts for technical clarity. Despite that fact, major efforts have been made to keep critical details or limitations concerning current developments of the field of quantum computing at the cost of arbitrary declaration (all referenced) without technical justification.

In fine, even considering current optimist trends of quantum computing development, **we cannot predict yet the viability of the technology** in the near future and advise a reasonable amount of skepticism toward that field.

References

[1] Quantum computing for computer scientists, N. Yanofsky and M. Mannucci, Cambridge Press, 2008.

[2] A. Kyrillidis's blog posts (https://akyrillidis.github.io)

[3] Berkeley University's CS191x Lectures

[4] St Petersbug State University's "The Introduction to Quantum Computing" Lectures on Coursera

[5] Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505510 (2019). https://doi.org/10.1038/s41586-019-1666-5

[6] Peter Shor. 18.435J Quantum Computation. Fall 2003. Massachusetts Institute of Technology: MIT OpenCourseWare, https://ocw.mit.edu. License: Creative Commons BY-NC-SA.

[7] Feynman, R. P. Simulating physics with computers. Int. J. Theor. Phys. 21, 467488 (1982)

[8] Shor, Peter W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing 26.5 (1997): 14841509. Cross ref. Web.

[9] Cristian S. Calude and Elena Calude. The Road to Quantum Computational Supremacy.arXiv:1712.01356, Dec. 2019.

[10] S. Aaronson. The limits of quantum. Scientific American, March:6269, 2008.

[11] Cook, Stephen (1971). "The complexity of theorem proving procedures". Proceedings of the Third Annual ACM Symposium on Theory of Computing. pp. 151158. doi:10.1145/800157.805047.

[12] E. Bernstein and U. Vazirani. Quantum complexity theory. In Proceedings of the 25th Annual ACM Symposium onTheory of Computing, San Diego, California, May 16-18, 1993, pages 1120. ACM Press, 1993.

[13] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven.Characterizing quantum supremacy in near-term devices.arXiv:1608.00263[quant-ph], April 2017.
[14] Boixo, S. et al. Characterizing quantum supremacy in near-term devices. Nat. Phys. 14, 595 (2018).
[15] Grover, Lov K. Quantum Computers Can Search Arbitrarily Large Databases by a Single Query. Physical Review Letters 79.23 (1997): 47094712. Crossref. Web.
[16] , Lov K., A fast quantum mechanical algorithm for database search,Proceedings of 28th Annual ACM Symposium on Theory of Computing, May 1996, pp. 212 219
[17] Dunjko, V., Briegel, H. J. (2018). Machine learning artificial intelligence in the quantum domain: a review of recent progress. Reports on Progress in Physics, 81(7), 074001. doi:10.1088/1361-6633/aab406
[18] Brown, K. L., Munro, W. J., and Kendon, V. M. 2010. Using quantum computers for quantum simulation. http://arxiv.org/abs/1004.5528.
[19] Nielsen, M. A., and Isaac L. Chuang. Programmable Quantum Gate Arrays. Physical Review Letters 79.2 (1997): 321324. Crossref. Web.
[20] Dan E. Browne and Hans J. Briegel. One-way Quantum Computation - a tutorial introduction, 2006.
[21] T. ALbash, D.A. Lidar, Adiabatic Quantum Computing, 2016.
[22] Lahtinen, Ville, and Jiannis K. Pachos. "A short introduction to topological quantum computation." SciPost Physics 3.3 (2017).
[23] Resch, Salonik, and Ulya R. Karpuzcu. "Quantum computing: an overview across the system stack." arXiv preprint arXiv:1905.07240 (2019).
[24] Krantz, P. et al. A Quantum Engineers Guide to Superconducting Qubits. Applied Physics Reviews 6.2 (2019): 021318. Crossref. Web.
[25] Bruzewicz, Colin D. et al. Trapped-Ion Quantum Computing: Progress and Challenges. Applied Physics Reviews 6.2 (2019): 021314. Crossref. Web.
[26] Gavin K. Brennen, Carlton M. Caves, Poul S. Jessen, and Ivan H. Deutsch. Quantum Logic Gates in Optical Lattices, Phys. Rev. Lett. 82, 1060 Published 1 February 1999
[27] Fedichkin, Leonid, Maxim Yanchenko, and K. A. Valiev. "Novel coherent quantum bit using spatial quantization levels in semiconductor quantum dot." arXiv preprint quant-ph/0006097 (2000).
[28] Longdell, J. J., M. J. Sellars, and N. B. Manson. "Demonstration of conditional quantum phase shift between ions in a solid." Physical review letters 93.13 (2004): 130503.
[29] Janus H. Wesenberg, Klaus Mlmer, Lars Rippe, and Stefan Krll. Scalable designs for quantum computing with rare-earth-ion-doped crystals, Phys. Rev. A 75, 012304 Published 3 January 2007
[30] N. A. Gershenfeld, I. L. Chuang, Science 275, 350 (1997)
[31] The Usefulness of NMR Quantum Computing, Warren S. Warren
[32] Diamond Sparkles in Quantum Computing, Aps Physics Volume 17, Number 5 (2008)
[33] Cavity Quantum Electrodynamics and Circuit QED: from Fundamental Tests to Quantum Information, Serge HAROCHE, (2016)
[34] Todd B. Pittman, Bryan C. Jacobs, James D. Franson. Quantum Computing Using Linear Optics. (2004).
[35] Burell, Zachary. "An Introduction to Quantum Computing using Cavity QED concepts." arXiv preprint arXiv:1210.6512 (2012).