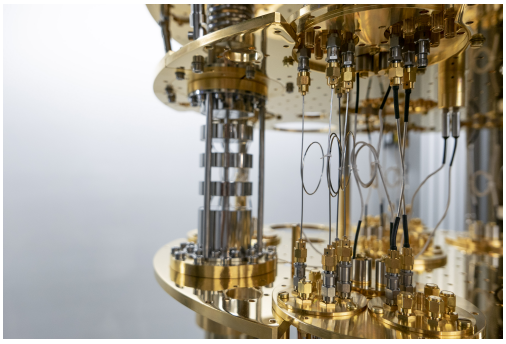

Department of Physics
UNIVERSITY OF STRATHCLYDE

MSC ADVANCED PHYSICS



# The mystery behind Quantum Computers

Ayush

Supervisor
Dr. Stefan Kuhr

2022

**Abstract**

Quantum computing has a notion of being something the most difficult system to understand and thus there is a need to explain the quantum computing field in an elaborative manner. An explanation of the need for quantum computing enables the development of different algorithms and models for a different kinds of computing. Moreover, we discuss the companies that are working in this field, their achievements and their goals for developing a quantum computer. Adding to this, we discuss the obstacles in developing a new type of technology altogether and conclude with comprehending the probable significance of a new technology i.e. Quantum Computing.

**Acknowledgements**

I owe a great debt of gratitude to Dr. Stefan Kuhr for suggesting me to write this report which enabled me to learn a lot about quantum computing. I have learned a great deal as I was offered guidance and thoughtful training. I would also like to thank him for putting up with my endless questions and am confident he will move the research forward and be succesful. Also, I would like to Dr. Thorsten Ackerman and all my teachers at Strathclyde for their continuous support, guidance and patience.

# Contents

# List of Figures

# Chapter 1

# Introduction

Classically, computers work on the principle of a classical bit where a bit is either in 1 or 0 depending on the current value for a transistor i.e. a switch. When we have 8 bits together, they make 1 byte which is considered to carry information, also called a byte a memory. These bytes contain a single piece of data and multiple bytes can contain a lot of information. Now, the purpose of a computer is to store memory and apply operations on these bytes to get different computation results. These tasks are accomplished using logic gates like the AND gate, OR gate, NOT gate, etc. Then, algorithms are built which define the order of the logic gate operations to provide a specific result. These computers are very good in accomplishing everyday tasks but a standard computer is capable of accomplishing only one task at a time (serial processing), which limits their processing speed for heavy load tasks like predicting the weather. This gives rise to the process of parallell processing, i.e. the process of slitting the task into chunks and each processor works on a specific chunk, which accelerates the process of computing exponentially. This principle is used in the functioning of supercomputers where parallel processing takes place at a massive scale, e.g. Sunway TaihuLight supercomputer had around $40,960260 = 10,649,600$ processor cores in July 2020. Although this process can produce lucrative results, there is a challenge of effectively dividing the workload and then assempling the partial results to get the final result. We can use Amdahl's law to determine the theoretical speedup we can expect using parallel computing. While the performance of supercomputers is usually operated in million instructions per second (measured in floating point operations per second), they become larger in size and the efficiency of an individual unit of a supercomputer remains lmited. Moreover, Intel Corporation's co-founder Gordon Moore came up with Moore's law, (he made an observation in 1965 while working on Fairchild semiconductor: the number of transistors placed on a microchip doubled that year), that the actual growth of transistor density doubling reduces in relative time behaving exponential in nature. Although it didn't take into account the increase in complexity and thus, each process node is now delivering less dramatic results in terms of density, performance and power reduction. To remedy this, Synopsys's co-CEO Aart de Geus came up with the term SysMoore to blend Moore's law with systematic complexity. Even then, the demands of the design are much greater than the improvement in the transistor technology we use now. Moreover, with the advent of machine learning and artificial intelligence, we need to compute much larger amounts of information in a short period of time as we create neural networks between computer systems to process much complex systems. Therefore, there is a great need for a different method of computing, which gives rise to a new method of computing in the form of Quantum Computing.

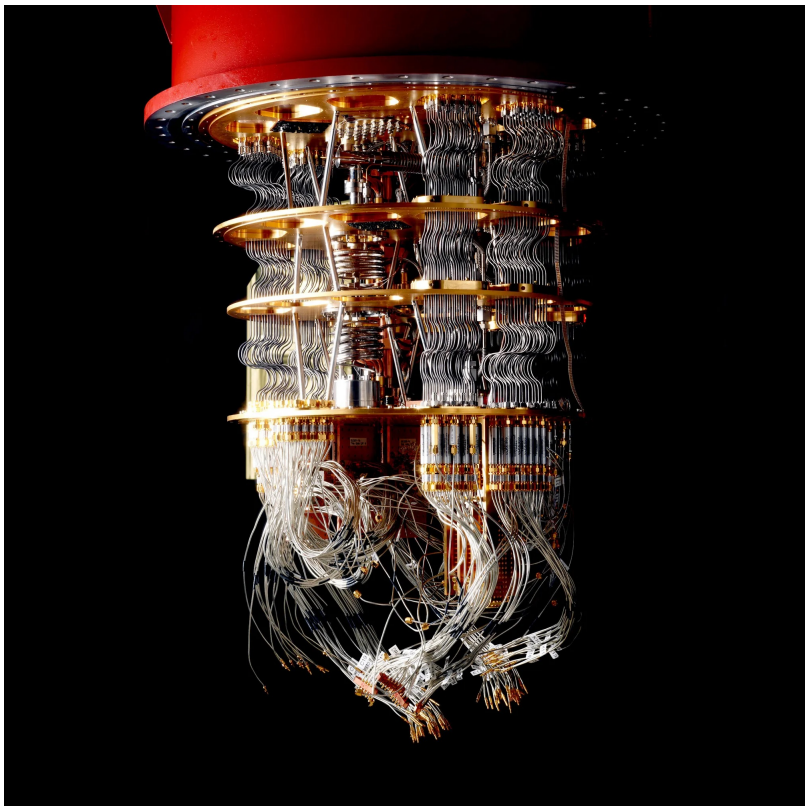


Figure 1.1: Sycamore Quantum Computer

## 1.1 Rise of Quantum Computing

There were many advancements in the fields of physics in the 19th century, significant being the study of electrical and magnetic fields and the realization of light as an electromagnetic wave. This gave us the realization of wave and particle nature of light which was extended to matter as well. As Schrödinger used the De Broglie's electron wave postulate to develop a wave equation for matter waves in 1924, the understanding of the fundamental nature of the universe was studied by the creation of the field of quantum physics. There were many developments in quantum physics and its applications in different technology was also studied across time. With theoretical applications in qauntum cryptography and quantum computations, it was extensively studied and experimented in labs but it was not known if it was possible to implement these theoretical realizations for real life applications. As Google declared quantum supremacy by publishing a paper in Nature in 2019 by creating a true random number using 52 qubits, the quantum race was established where multiple companies and countries work extensively to build a practical quantum computer for general use. As quantum technology opens up a different approach to our understanding of computing we need to understand the respective principles that undertake the building of a quantum computation.

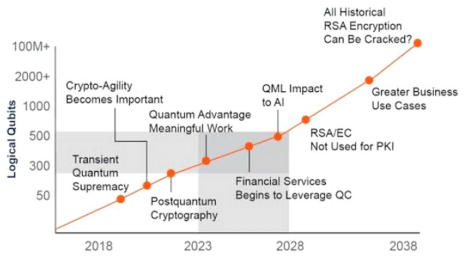



Figure 1.2: Potential rise map for quantum computers

Some of the significant achievements towards quantum computing that have been described by the University of Oxford are as follows:
1900 - Max Planck publishes "quantum theory"
1905 - Einstein proposes "quantum of light"
1913 - Niels Bohr formulates "atomic structure based on quantum principles"
1932 - John Von Neuman created "hilbert space formalism of quantum mechanics"
1947 - electromagnetic properties of electrons, positrons and photons - feynman diagrams
1957 - Theory of superconductivity by John Bardeen, Leon Cooper, and Robert Schriefer at the University of Illinois - Noble Prize 1972
1960 - Stephen Wiesner introduced "conjugate coding"
1964 - Nikolai G Basov and Aleksandr M Prokhorov - Nobel Prize in Physics 1964 for "semiconductor laser and quantum electronics"
1973 - Charles H Bennett - IBM research - "reversible computation"
1976 - Roman Stanislaw Ingarden formulates "quantum information theory"
1981 - Richard Feynman proposed the basic model of quantum computer
1985 - David Deutsch describes the first universal quantum computer
1991 - Arthur Ekert invents "entanglement-based secure communication"
1994 - Shor's algorithm for security
1998 - Jonathan A Jones and Michele Mosca build "first ever working 2-qubit NMR quantum computer for Deutsch's problem"
2001 - first execution of Shor's algorithm at IBM's Almaden Research Center and Standford
2004 - first working pure state NMR quantum computer at Oxford and York
2005 - first "quantum byte" created in Innsbruck, Austria & creation of quantum memories
2006 - qubit stored in a stable buckyball
2006 - first 12 qubit quantum computer
2011 - two diamonds linked together in entanglement
2014 - Oxford's ion trap set world record for highest fidelity control of any qubit (single - 99.9999%)(two-qubit - 99.91%)
2016 - IMB free service launch for 5 qubit quantum processor over it's cloud
2018 - Oxford breaks speed records for building blocks of quantum computing
2019 - IBM Q system one allows quantum calculations over the internet
2019 - Oxford doctoral student with MIT and IBM develop and test a quantum algorithm for machine learning, showing how quantum computers will be able to map data at a far more sophisticated level than any classical computer.

## 1.2 What is quantum computing?

Quantum computing is the type of computing which might be an active solution to our problem as it takes a complete different approach towards computing in the fundamental sense. Although the field of quantum computing began in 1980 with the modelling of the Turing machine quantum mechanically by physicist Paul Benioff, it gained prominence with Richard Feynman's paper "Simulating Physics with Computers" in 1982. In 1998, the first two-qubit quantum computer was developed that could perform computations but it was believed that a fault-tolerant quantum computer was a pipe dream until Google with NASA declared supremacy. In terms of quantum computations, the whole apparatus of computing changes dramatically, where qubits are now the basic memory units, quantum logic gates are used to operate on these qubits, and distinct quantum algorithms have to be made now to simulate desired results.

The main advantage of a quantum computation over a classical computation is that it can hold multiple states at a particular time as sooposed to a classical computation where only one state can be held at a particular time. This type of behaviour is achieved using three principles of quantum physics: superposition of states, entanglement between qubits and interference of quantum-mechanical waves. Moreover, the quantum logic gates have the same number of inputs and outputs and the quantum algorithms are made in such a way that the input parameters can directly take the state of the real life variable and the output can be computed without computing all possible combinations.

## 1.3 Need for quantum computers

The first thing we need to understand is that quantum systems are unable to be comprehended on a macroscopic scale and we need a system to represent the quantum systems. Thus, they are unable to input or output any information, thereby have no capability for controlling real time devices. Thus, we need to develop a system in which we provide classical messages to an interface which then converts our system into a quantum system which can then provide a classical result to us by the measurement of the quantum system. Since we develop a complete new type of technology, we need to understand the potential applications of quantum computers. As we understand these systems, we came with two major problems where they might provide effective solutions:

1. Quantum Simulation problems -
   In terms of simulation of real life systems, we need to take into account a lot of factors and computing all the possible outcomes is a tedious job, thus quantum computers can perform solutions to real-life problems efficiently. We noticed that simulating even 30 particles is difficult for the fastest superconductors and quantum computers bring promise for such problems. Examples - Simulations of chemical reactions, or How electrons behave in different materials , Ferilizer effect on global warming, Improving solar panels and batteries, Drug development, Improving materials for aerospace and new chemicals. Simulating only 30 particles is difficult for the fastest supercomputers

2. Optimization problems -
   Quantum computers show great potential in solving optimization problems i.e. the problems where a lot of data is inputted to create an algorithm for finding the best optimized path for a problem.
   Examples - Machine learning, Artificial Intelligence, Financial modelling, Weather forecasting

3. Cybersecurity -
   Quantum physics allows for creating a key that doesn't exist in physical state unless it is measured which enables creation of secure keys that can used for secure cyptography purposes.

# Chapter 2

# Quantum Circuit

Here, we would like to understand the basic memory units in a quantum computer and how it interacts for computations. We also discuss the different models developed to physically realize these quantum computations. We develop the basic understanding of a quantum circuit which might form an underlay platform for the development of performing quantum computations.

## 2.1 Hilbert Space

It is an inner product space that is complete with respect to the norm defined by the inner product. In simple words, it is the space where the quantum vectors live, i.e. the set of all values of a quantum state. In physical terms, it can be seen as the surface of the Bloch sphere which contains all the values to which a vector defines a quantum state.

It is a very important pheneomenon to be understood as it defines the complex vector space that we work on, for quantum computation.

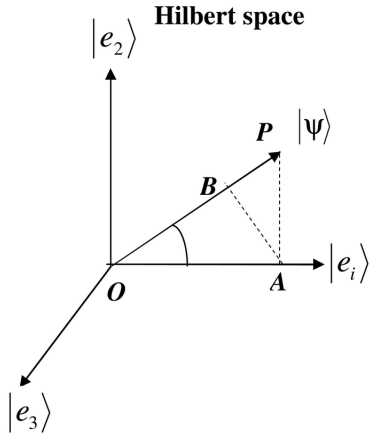



Figure 2.1: Hilbert space representation

With comparison to classical computation, we can make a analogy to the set of real number, i.e. it is the set of all values for a qubit similar to a value being a set of real number of sets of $\{0, 1\}$.

## 2.2 Qubits - Memory

A qubit is the fundamental unit of quantum information which can be elaborated as a two-state quantum mechanical system (simplest form of a quantum system), and can be represented as a superposition of the two states of the quantum mechanical system.

Physically speaking, in terms of quantum physics, every elementary particle is a quantum mechanical wave and consequently, a qubit can be represented as a quantum mechanical wave in a quantum harmonic oscillator with only two energy states. Thus, a qubit exists in only these two states and the solution of such a system is represented in a manner to portray as a function of the probabilities of the two states.

Therfore a pure qubit state is a coherent superposition of its basis states. If we represent these two states as vectors to exhibit the behaviour in terms of digitial bits for computations, we create vectors $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. and a single qubit being the linear combination of these states represented as

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

where $\alpha$ and $\beta$ are the complex probability amplitudes for the states $|0\rangle$ and $|1\rangle$ respectively. Since the probability of the two states are exhaustive for a pure qubit, the normalization constraint can be written as

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

which then gives us 3 degrees of freedom and we can represent in 3d space using a Bloch sphere.

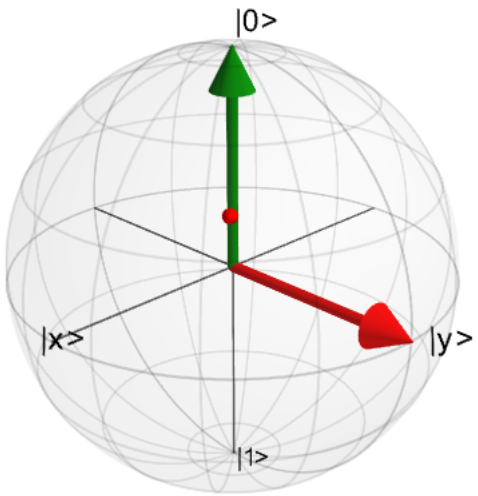



Figure 2.2: Bloch sphere representation of a pure state

Therefore, the actual state can be represented visually in the form of a surface point on a Bloch sphere where the poles can be the two definite states, and the probabilities can be plotted as

$$\alpha = \cos\frac{\theta}{2}$$

$$\beta = e^{i\psi} \sin \frac{\theta}{2}$$

where $e^{i\psi}$ is the relative phase significant for representation and $\theta$ is representation to the possible quantum state.

Important Note:
We see that a pure state is essential for creating a useful qubit since the quantum state and the probabilities can be known easily and there is a need for representation of a mixed state qubits to be statistical combined to form pure states. Thus, a mixed qubit state needs another degree of freedom i.e. the length r of the vector to represent the mixed state. A mixed state is physically by the points inside the Bloch sphere and in case of qubits, we have only two quantum states, it can be represented as a Poincare Bloch ball in terms of a qubits.

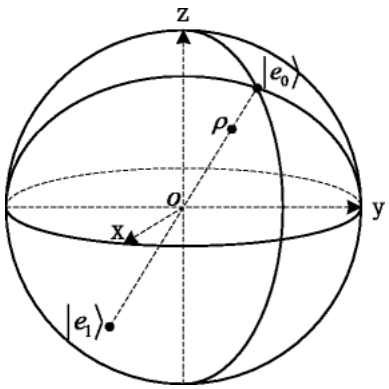



Figure 2.3: Bloch sphere representation of a mixed state

## 2.3 Models for Quantum Computations

Now we have described the basic memory unit in a quantum computation, i.e. qubit, we need to describe to propose a method for interaction of these qubits to perform computations. To achieve this, researchers have developed different models for applying interactions between these qubits quantum mechanically to get the results which are realized through quantum measurement which collapses the quantum function to a classical result. We understand that computational reversibility is necessary for increasing the computation power as it is directly related to energy consumption and heat dissipation. To produce reversibility in classical machines, you need two operations to be carried out. While a fundamental principle of quantum physics is that every change is reversible. Some of the most popular models created for quantum computations are:

- Gate based Quantum Computing -
  This model is based on the principle of classical computing where logic gates are used for operating on the bits to get a result. In our case, a quantum circuit would be constructed where qubits interact with each other using quantum logic gates and based on these gates and the algorithm of the quantum circuit, the computation takes place.

- Measurement based Model -
  This model is similar to a Gate based model with the use of a quantum circuit but this model does only one-way quantum computing. Here, The entangled state is set up according to

the quantum circuit and then measurement of each qubit is done during computation and mathematically return the same values as the gate model.

- Adiabatic Model -
  This model works on the principle that any quantum system tends to result in a state with the lowest energy. Therefore, the computation problem is set up in such a way that the result of the computation would fall on the lowest energy state. Here, an energy landscape is basically created according to the the quantum system and the lowest energy state returns the result of a computation. This model is based on the nature's own principle and thus runs on a universal quantum scheme, i.e. it can run any quantum system. Even though the approach of this model is completely different, it is mathematically equivalent to the circuit model.

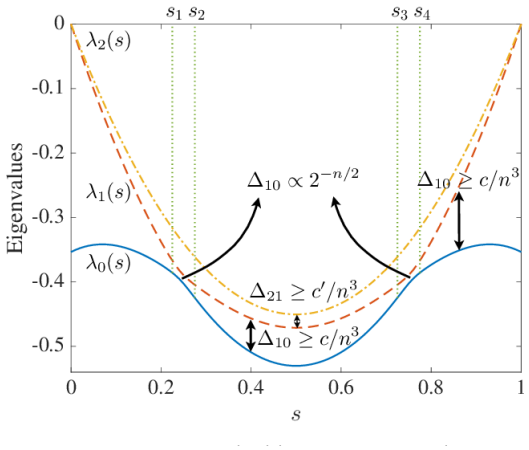



Figure 2.4: Energy level for adiabatic computing

- Quantum Annealing Model -
  This model is similar to the adiabatic model but it doesnt allow for full degrees of freedom. Although this model is not universal in nature, it is used for specialized purposes like optimization problems and simulation problems. This model works as a stepping stone to creating a complete adiabatic type approach to quantum computing.

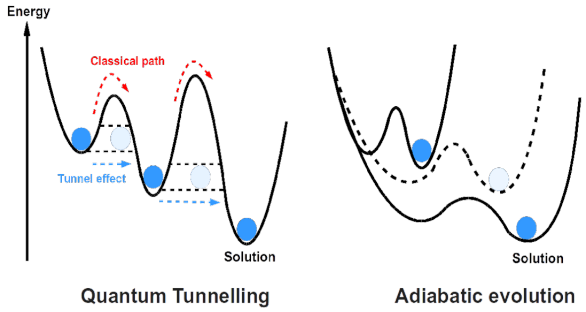



Figure 2.5: Quantum annealing effect

- Topological Quantum Computing -

This approach to quantum computing has not been realized in any sense till now and is thus the most theoretical approach till date. Here, the qubits are made of majorna zero-mode quasi-particle which is a non-abelion anyon. A quasi particle can be considered as a stable qubit as it is a collection of fundamental particles that behave as a single particle and the major advantage of a quasi-particle is that it is protected from rogue energy that enters the quantum system by the energy gap between the fundamental particles (threshold energy needed to overcome the energy gap).

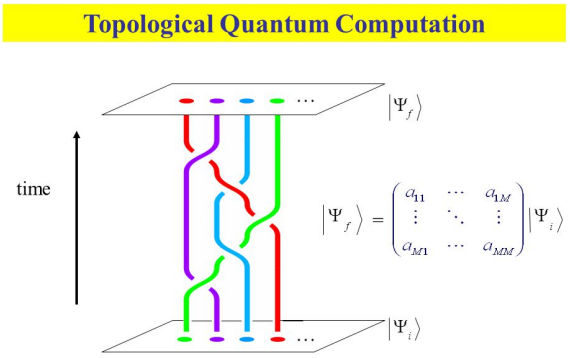



Figure 2.6: Topological computing representation

## 2.4 Components of a Quantum Circuit

Now we need to implement these algorithms using a quantum computer and thus need to understand the hardware components of a quantum computer. We need to build a computer for interface with users, data, and networks like a conventional computer. Although it is active field of research, we can state the essentials components for building the hardware structure of a quantum computer:

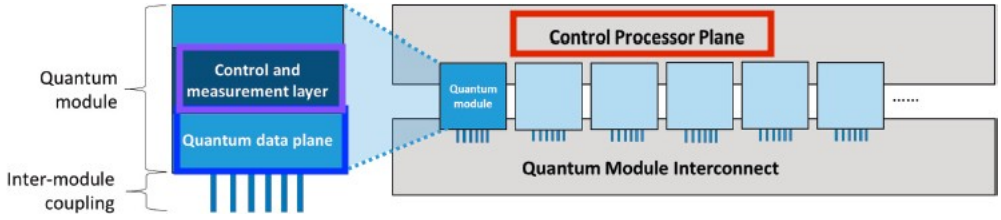



Figure 2.7: quantum circuit components

- Quantum Data plane -
  This is the heart of quantum computation. This plane contains the physical qubits and the structures to hold these qubits. Also, the support circuitry to measure the qubits' state and perform gate operations (or control the Hamiltonian) is a part of this plane. Physically, this component contains the quantum housing and the quantum chip as well as the wiring required for computation.

- Control and Measurement plane -
  This plane consists of converting the control processor's digital signal to convert to actions of the quantum logic gates. This basically performs the operations on the qubits according to the respective algorithm.Moreover, the goal of a quantum computation is to transfer the quantum state to the user and thus, this plane may consist of a quantum router and a quantum repeater for transfer of quantum state over a long distance.

- Control Processor Plane and Host Processor -
  This plane bridges the gap between classical input/output phase that interacts with the user, and the quantum computations needed for the solutions to the problems. This contains the processor that gives the commands to execute a program.

While constructing a quantum circuit comparable to a classical computer, we take the approach of the gate model and thus the need to construct a quantum circuit arises. Using qubits as memory, we understand that a quantum circuit uses a fundamental different principle compared to a classical computer circuit and thus we use various quantum logic gates to produce operations or interactions between these qubits. This causes interference of the quantum mechanical waves and a special case also arises in the case of quantum physics, i.e. entanglement, where the behaviour of one qubit gets entangled with the other qubit to produce interesting results.

## 2.5 Quantum Logic Gates - entanglement and interference

Now, to understand the flow of computation in a quantum circuit, we use different quantum logic gates to apply different operations on the qubits, the interactions between these qubits result in changing the quantum state of these qubits. The special property about quantum logic gates is that they have the same number of inputs and outputs unlike classical bits where the result of operation is linear in property.

Logically speaking, applying logic gates in a quantum circuit is equivalent to applying an operator function on the quantum state to modify it to perform computations.

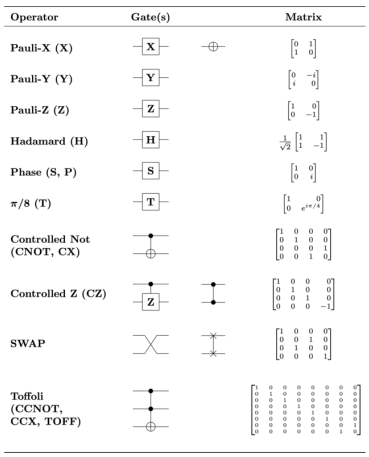



Figure 2.8: Common Quantum Logic Gates

There are a few basic quantum logic gates that are used generally to make quantum circuits:

1. Pauli gates - based on the pauli matrices

   The most basic quantum gates can be the gates that apply unitary operations on the qubit. As we represent a qubit in the form of a Bloch sphere, we can Pauli matrices or the unitary matrices in the x, y, z direction to rotate a single qubit to change its state. These matrices are represented as:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

   These are constructed in such a way that they create a rotation of $\pi$ along the three axes of the Bloch sphere respectively and thus they are their own inverse resulting in the identity matrix when squared.

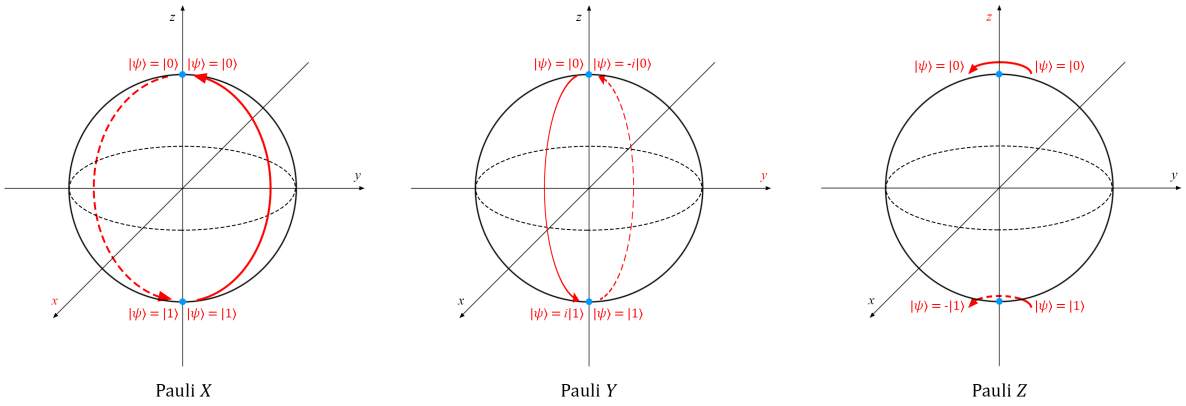



Figure 2.9: Pauli gates for bloch spheres

   Since Pauli-X flips the qubit about the x-axis, it flips the bit value and thus can be termed the NOT gate or bit-flip gate. Similarly Pauli-Z flips the phase of the qubit by rotating about the z-axis, it is called the phase -flip gate and it can be modified to produce phase-sift gate to rotate the qubit by a particular angle.

   Since we see that these functions are exponential in nature, the $n^{th}$ root of these quantum gates result in $\pi/n$rotation about the respective axes, and can create a square root function for rotation of $\pi/2$ about these axes. hermitian

2. Hadamard Gate

   Since we have a vector in 3d space, we would like to know the inverse of the vector, i.e. rotating the vector in the exact opposite direction of the initial vector. Thus , we make a rotation about the axis $\frac{(x+z)}{\sqrt{2}}$ to form the Hadamard gate. The Hadamard matrix is thus described as:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

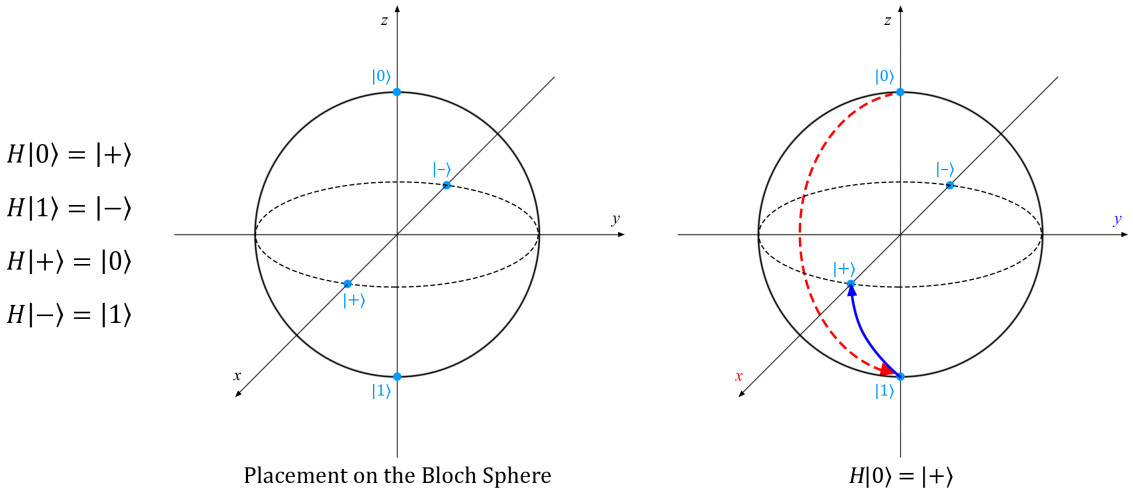



Figure 2.10: Hadamard gate for bloch spheres

It is a form of unitary involutary transformation and can be also written as $H = R_y(\pi/2)Z = XR_y(\pi/2)$. Here, also, we can create specific rotations about the $\frac{(x+z)}{\sqrt{2}}$ axis by taking the $n^{th}$ root of the Hadamard gate. hermitian

3. Controlled Gates

   A controlled gate is the special gate in quantum information where qubit 1 influences qubit 2 to cause a rotation in qubit 2. (This is not observed in classical computation as all bits are independent from each other which is not the case with qubits). It acts on two qubits in such a way that the first qubit serves as a control and this gate is represented as:

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

   where U is the unitary transformation to be produced on qubit 2 where

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

   Thus, the 1st qubit can control the unitary operation to be applied on qubit 2 and it can multiple pplications.

4. Swap Gate

   As the name suggests that this gate might swap the quantum state of the two qubits but this is not true. To understand this gate, we must realize that we are not concerned about the individual quantum state of a qubit and are only concerned with the measurement of the state. This can roughly be translated to a situation where we are just concerned if that bit in the northern hemisphere or the southern hemisphere of the Bloch sphere, because that state is the one which will be measured. So the measurement states of the two qubits in SWAP

gate is swapped but the individual probabilities for a specific qubit gets swapped with each other. Thus, this gate swaps the quantum state of a qubit on itself with relation to the state of the other qubit and this gate can be constructed using a combination of 3 CNOT gates swapping the computation measurement states of the two qubits. It is represented as:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

As we understand the SWAP circuit is a conditional rotational of the qubits along the x-axis, we can also produce this rotation at a different angle by taking the fractional exponents of the SWAP gate. Thus, $\sqrt{SWAP}$ can be made to perform halfway of swap, i.e. the controlled gate at an angle of $\pi/2$, which can be defined as:

$$\sqrt{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{\frac{i\pi}{4}} & \frac{1}{\sqrt{2}}e^{\frac{-i\pi}{4}} & 0 \\ 0 & \frac{1}{\sqrt{2}}e^{\frac{-i\pi}{4}} & \frac{1}{\sqrt{2}}e^{\frac{i\pi}{4}} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

5. Special Quantum Gates In a classical computer, you cannot produce different logic gates but can only place the logic gates in a particular sequence for desired results. Quantum circuits allow for the creation of new quantum logic gates with simultaneous operations on qubits because of the dependency of the one qubit on the other by controlled gates. Here, these gates can then be used for interdependence of the qubits which opens new possibilities for quantum bits in the fundamental sense. Some of these kinds of popular quantum gates include:

   - Deutsch Gate

     The Deutsch gate is a gate where an angular rotation about the x-axis is controlled by the 2 other qubits. Thus the general form of the matrix for Deutsch gate can be written as:

     $$|a, b, c\rangle = \begin{cases} i\cos\theta\,|a, b, c\rangle + \sin(\theta)\,|a, b, 1-c\rangle\,, & \text{for } a = b = 1 \\ |a, b, c\rangle & \text{otherwise} \end{cases}$$

     One special case for angle $\pi/2$ is the Toffoli gate or CCNOT gate which can be shown as:

     $$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

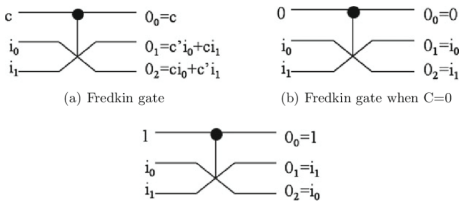
     This gate is special as it can be related directly to the classical AND and XOR logic gate operations.

- Fredkin(CSWAP) Gate

  The CSWAP gate is a special gate that performs the SWAP operation which is controlled by a 3rd qubit, which is represented as:

$$CSWAP = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

  This gate has high significance as it can help in computing a controlled swap and the number of 0s and 1s are conserved throughout.



(a) Fredkin gate (b) Fredkin gate when C=0

Figure 2.11: Fredkin gate

- Other Combinations for Quantum Logical Gates

  We can produce many other quantum gates for selective needs according to our needs with the use of these basic logic gates keeping in mind that they are universal in nature, i.e. they can perform operation on any quantum state. Some of these gates include the ising coupling gates, imaginary SWAP gate, etc.

## 2.6 Computations on quantum logic gates

After understanding the quantum gates and their operations on the qubits, we need to understand the computations in a circuit. In a general sense, the connections can be made either in a series configuration or a parallel configuration. While in classical circuits, the computation follows the current flow and thus series gates pattern is followed and parallel current flow doesnt matter, it is not the case with quantum circuits because of superposition of quantum waves behaviour.

- Serial configurations

  When two gates A and B act on n qubits, the resultant effective matrix of the two gates can be described as the matrix multiplication of the two matrices.

$$C = B \cdot A$$

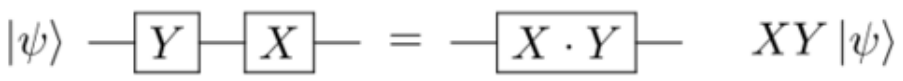



Figure 2.12: Series connection

This is thus used for producing exponents of a quantum gate and applying different computations on a qubit in a particular order for a desired result, i.e. altering the probability distribution of the qubit for aspired outcomes.

- Parallel configurations

  While classical logic gates act upon the difference in voltages, they have no effect on parallel configurations, quantum logic gates are a bit different and the quantum mechanical waves interfere with each other to give a resultant matrix as the tensor product or Kronecker product of the two individual quantum gates.

$$C = B \otimes A$$

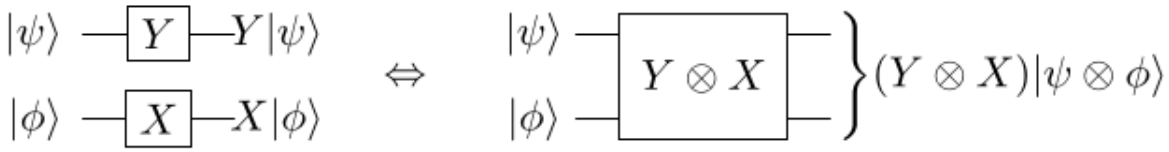



Figure 2.13: Parallel connection

We can understand that even parallel gates can result in influencing the outcome of the result and a signal without a gate can be considered as an identity gate, thus the final state is basically formed as a result of interference of the two qubits, which can also result in the influence as entanglement of the two qubits where their natures depend on each other.

NOTE : One of the essential problems with a quantum computer also arises due to this reason, i.e. the emergence of noise due to the interference of the quantum mechanical waves with the surroundings.

## 2.7 Special Computations

### 2.7.1 Unitary Inversion of Gates

Since we know that all quantum gates are reversible, any composition of these gates can also be proven to be reversible. Thus, for any unitary matrix, there exists an inverse unitary matrix to give an identity matrix, i.e. the original quantum states for the qubits.

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

Also a function as a combination of series gates and parallel gates can simply be described respectively as:

$$F^\dagger = (\prod_{0\leq i\leq m} A_i)^\dagger = \prod_{0\leq i\leq m} A_{m-i}^\dagger$$

$$G^\dagger = (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$$

This allows for computation and uncomputation as well, and can be applied as function inversions in quantum programming concepts. Also the gtes which are their own unitary inverses are called Hermitian operators and can be used extensively in computing.

### 2.7.2 Entanglement

These quantum gates can produce very effective results using the phenomenon of interference of individual qubits. While this is helpful for computation, there is an interesting phenomenon that takes place with interference of the qubits when the resultant on these qubits ia entangled with each other. This is the feature that sets quatum computation far superior than classical computing. Since, when the qubits might be entangled, a single measurement can be made on one qubit which collapses the other qubit into a specific configuration as well, giving us information about the other qubit without measuring it (thereby it looks like information has travelled faster than the speed of light - applications in quantum teleportation).

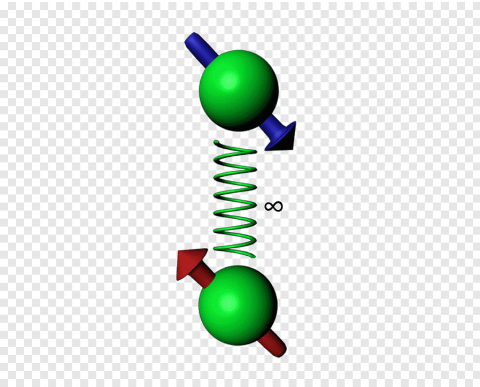


Figure 2.14: Entanglement of two qubits

One of the simplest circuits for creating entangled qubits is using the Hadamard gate on 1 qubit with controlled X basis gate for 2nd qubit and the resultant will be entangled,i.e. using H and CNOT gate, we can write this quantum circuit as follows:

$$F = CNOT(H \otimes I)\,|A\rangle \otimes |B\rangle$$

We can understand it with an example where we take an input state as $|00\rangle$ and the computation will result in

$$F\,|00\rangle = (\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}(\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\otimes\begin{bmatrix}1&0\\0&1\end{bmatrix}))\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

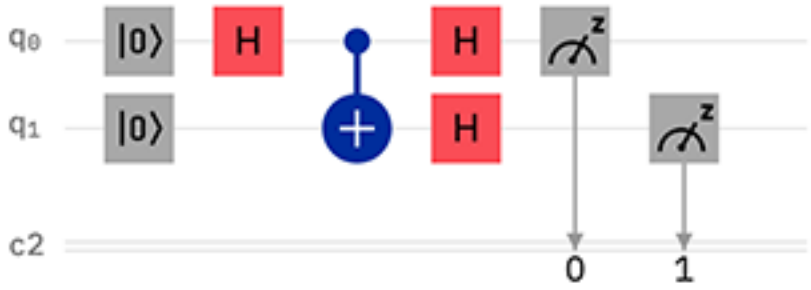



Figure 2.15: Basic circuit to create entanglement of two qubits

Here, we can observe that the resultant state gives $|00\rangle$ or $|11\rangle$ with equal probability, and if we measure just one qubit, we know that the other qubit state will be the same. This is one of the Bell states that can be formed using this configuration. Using the same configuration, we can change the input that can then result in giving us other Bell states.

With entanglement, we can see how quantum computations takes a leap forward in 3 specific areas:

- Superdense coding with information exchange that looks faster than light
- Quantum cryptography when a key encoded based on entangled photons
- Quantum teleportation where information can be transported to another place as one of the entangled qubits interacts with the information that needs to be transported

## 2.8 Measurement

We need to understand that the real form of a qubit is a quantum mechanical wave which is formed by the interference of quantum mechanical waves that were formed by the superposition of two quantum states, and the quantum state collapses to give a classical result when it is measured. Thus, it is an irreversible process that is carried on the qubits to return results. Technically speaking, the measurement plane defines the projection plane for the qubit along which we get a classical result according to the probability. In simple terms, if we represent the qubit by a vector in bloch sphere, the probability and measurement result is given by the measurement plane along which we find the projection of the bloch vector.

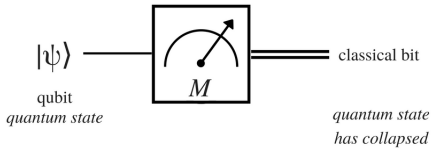



Figure 2.16: Qubit state measurement

In our case, we keep the measurement plane in the same basis as we use to create the quantum state for measurement can be done along the 3 planes for obtaining the measurement results. Classical results are obtained from the measurement plane, which if placed at an angle to the plane in which they were created can produce a different probibility distribution than when done in the same measurement plane as creation.

Logically, measurement of a quantum state is equivalent to applying an observable to the quantum state to determine the observable property of the quantum state. To visualize this, this observable basically determines the projection of the quantum state along the plane defined by the observable property.

For quantum computing, we can make registers of these qubits which be pairwise entangled with another registers paving way for much faster computations. Moreover, the measurement results are independent of the order of measurements made.

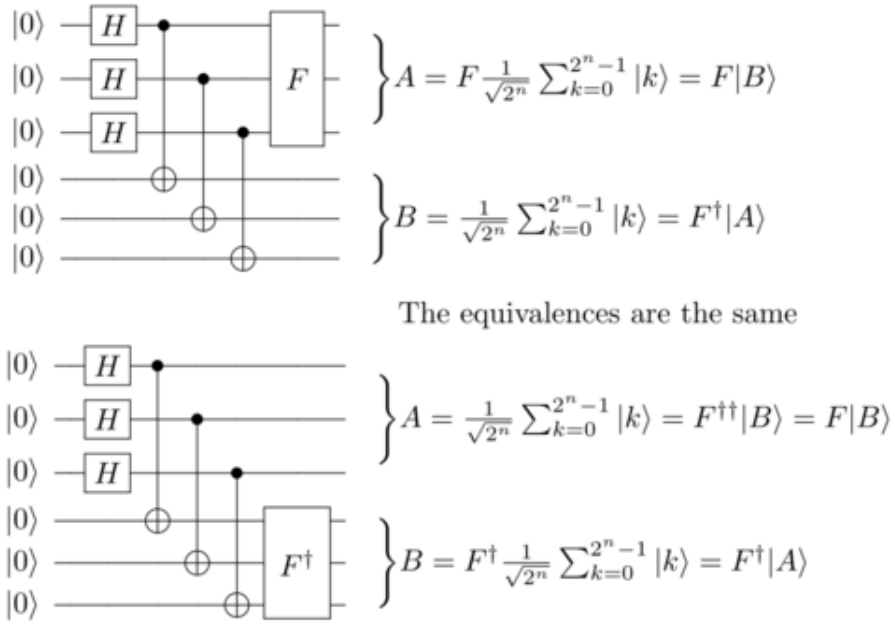



Figure 2.17: A basic quantum register

# Chapter 3

# Quantum algorithms

An algorithm is defined by a set of rules to perform problem-solving operations and thus after studying the basic quantum circuit, there is a need to develop different quantum algorithms to implement practical scenarios to compute results. These quantum algorithms basically define the process of computation steps that we can use for a particular type of problem. Since, quantum computations take a completely different approach to the steps involved in computing a problem, we define quantum algorithms for various kinds of problems. These algorithms also portray the different potential uses of a quantum computer.

(Note: Although we form quantum algorithm based on the GATE model, they can be stated similarly in other models of computation, like the Hamiltonian oracle model)

With the computational complexity theory, we can understand the complexity of a problem and can classify a specific problem accordingly. This classification helps us to determine the algorithm to be applied for that particular computation. Computational problems are classified according to their resource usage and how these classes are related to each other, which depends on the factors: type of computation (function problem, counting problem, optimization problem, etc.), model of computation (deterministic Turing machine, non-deterministic Turing machines, quantum Turing machines, etc.), or the bound for resources (polynomial time, logarithmic time, constant depth, etc.). With this information, we introduce the common problem classification that we encounter:
P - problems solved in polynomial time
NP - problems verified in polynomial time
NP-complete - difficult problems in NP
PSPACE - problems that require polynomial amount of memory
BPP- problems that are solved in bounded-error probabilistic polynomial time

In terms of problems itself, the problems that can be solved quantum mechanically can be defined as BQP(bounded-error quantum polynomial time) or the problems that can be solved by a quantum computer. It was determined that the BQP problems are a superset of P problems and BPP problems(main difference being the additional input of r random inputs) but not NP problems, i.e. quantum computers can solve problems more difficult than problems solved in polynomial time(deterministic and non-deterministic(including probabilistic) problems) without verifying it, which make them really useful to interpret results without computation of all possible configurations.

To understand it simply, when we can define algorithms into two categories: deterministic and non-deterministic, i.e. the algorithms with a specific directional flow and the algorithms with a branchial flow. Moreover, we understand that P problems are a subset of BPP problems but not vice versa, i.e. the problems solved in polynomial time can be expressed as probabilistic problems,

but not the other way aound, e.g. Primes problem(whether a number is prime or not) is a problem in P that can be defined in BPP, but a problem like polynomial identity testing(whether two multivariate polynomials are identical - to determine whether a polynomial is equal to the zero polynomial if the arithmetic circuit is given) is a problem in BPP that has no resemblence in P. Thus, a quantum computer is efficient in solving both deterministic and probabilistic problems can therby different algorithms are produced to achieve these computations.

## 3.1 Algorithms based on quantum Fourier transform

We understand that a quantum logic gate results in an exponential function and thus we need to convert discrete values in a fashion that it can be implemented to quantum logic gates we studied. For these discrete samples of data, we convert them into a Fourier transform function and then implementation can be done by using a polynomial number of quantum gates. Thus, there are many algorithms based on the polynomial use for specific type of problems.

As we know that a discrete Fourier transform converts a finite sequence of equally-spaced samples of discrete-time Fourier transform. Thus this transform enables us to convert digital data to analog information (and vice versa using inverse fourier transform).

**Quantum Fourier transform**

The quantum Fourier transform is the quantum implementation of the discrete Fourier transform over the amplitudes of a wavefunction. It acts on a vector $(x_0, \cdots, x_{N-1})$ and maps it to the vector $(x_0, \cdots, x_{N-1})$ according to the formula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$$

where $\omega_N^{jk} = e^{2\pi i \frac{jk}{N}}$. Similarly, we can map it to a quantum state and make a unitary matrix for the same as:

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{jk} \left|k\right\rangle \left\langle j\right|$$

Figure 3.1: A general gate representation for fourier transform

The Fourier transforms in quantum computing can be visualized by the rotation along the imaginary plane where it makes the function a continuous one for discrete values for computation.

### 3.1.1 Deutsch-Jozsa algorithm

[9]

**Value:**

It is the first algorithm that shows the separation between the classical and quantum approaches in solving problems as a quantum amplitude can take both positive and negative values, while classical probabilities are always positive, and demonstrated the exponential behaviour of quantum computation.

**Problem:**

N bits of information is given and we need to know if the N bit register is **constant** (all inputs are either 1 or 0) or **balanced** (half of the bits are 1 and half are 0)

**Classical solution:**

If there are N bits, there are $2^N$ total number of outcomes.

For a Boolean function $f(x)$ made of N bits, $f(x_1, x_2, x_3, \cdots x_N)$ to be determined as constant or balanced, we need $2^{N-1}+1$ trial inputs to be certain that $f(x)$ is constant or not. So we are running the classical algorithm, the input has to go $2^{N-1}+1$ computations for 100% confidence to determine constant or not.

**Quantum solution:**

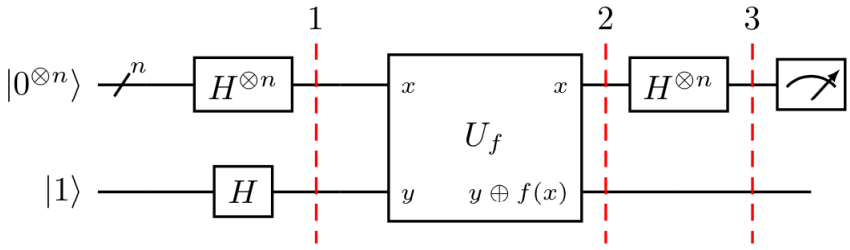



Figure 3.2: Deutsch Jozsa general representation

For a Boolean function $f(x)$ made of N bits, $f(x_1, x_2, x_3, \cdots, x_N)$ to be determined as constant or balanced, we can achieve the result in only one call if we use a quantum circuit. This algorithm has the following steps:

- Prepare two quantum registers. The first is an n qubit register initialized to $|0\rangle$, and the second is a one-qubit register initialized to $|1\rangle$

$$|\psi_0\rangle = |0\rangle^{\otimes N} |1\rangle$$

- Apply a Hadamard gate to each qubit:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{N+1}}} \sum_{x=0}^{2^N-1} |x\rangle (|0\rangle - |1\rangle)$$

- Applying the quantum oracle $|x\rangle |y\rangle$ to give $|x\rangle |y \oplus f(x)\rangle$:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{N+1}}} \sum_{x=0}^{2^N-1} |x\rangle (|f(x)\rangle - |1 \oplus f(x)\rangle) = \frac{1}{\sqrt{2^{N+1}}} \sum_{x=0}^{2^N-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

since for each $x$, $f(x)$ is either 0 or 1.

- Now, the second single qubit register may be ignored since it doesn't change, which is called the ancilla. So apply a hadamard gate to each qubit in the first register again to give us the solution.

$$|\psi_3\rangle = \frac{1}{2^N} \sum_{x=0}^{2^N-1} (-1)^{f(x)} [\sum_{y=0}^{2^N-1} (-1)^{x \cdot y} |y\rangle] = \frac{1}{2^N} \sum_{y=0}^{2^N-1} [\sum_{x=0}^{2^N-1} (-1)^{f(x)} (-1)^{x \cdot y}] |y\rangle$$

where $x \cdot y$ is the sum of bitwise product.

- Now just measure the first register. Now the probability of measurement of$|0\rangle^{\otimes N} = |\frac{1}{2^N}\sum_{x=0}^{2^N-1}(-1)^{f(x)}|^2$, evaluates to 1 if $f(x)$ is constant and 0 if $f(x)$ is balanced.

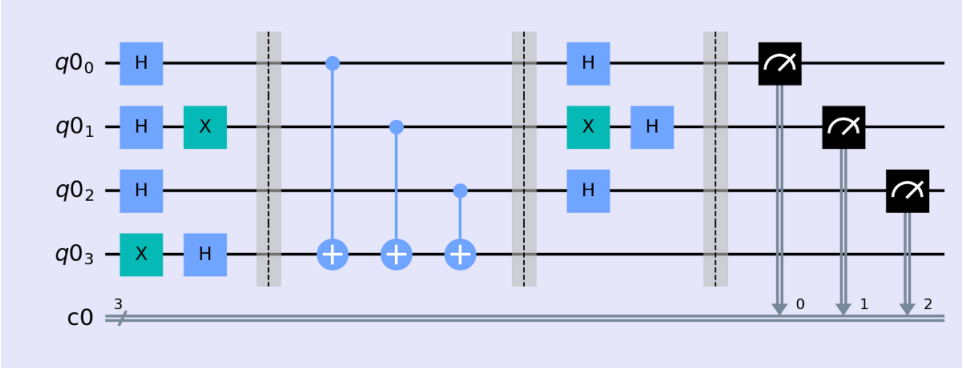



Figure 3.3: Deutsch Josza agorithm example for 4 qubits

### 3.1.2 Bernstein Vazirani algorithm

[23]

**Value:**

Building on the Deutsch-Josza algorithm, we would like to convert our considered problem into returning the value of a string as the function is checked if it is balanced or constant. So, we learn the value of the string encoded in a function and it can act as an oracle separation between complexity calsses BQP and BPP.

**Problem:**

To find the secret string s with N values.

**Classical solution:**

Here, given an input $x$, $f(x) = s \cdot x(mod2)$, we need to find s.

Here, we need to put 1 value for each bit individually and call the function to find each value of the secret string s. Thus, we need to run the algorithm N times for obtaining s.

**Quantum solution:**

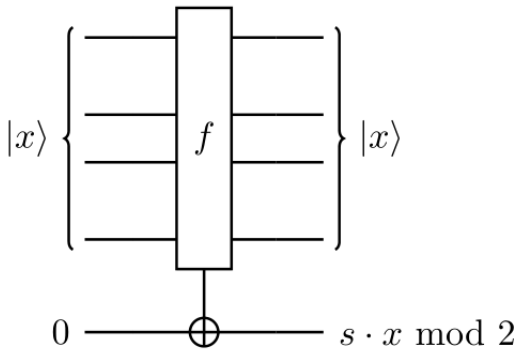



Figure 3.4: Bernstein Vazirani general representation

Here, the value of the string can be known in just one call using the the same principle as in Deutsch Josza algorithm and we follow the following steps:

- Initialize the input bits to the $|0\rangle^{\otimes N}$ state, and output qubit to $|-\rangle$
- Apply Hadamard gates to the input register

$$|a\rangle \xrightarrow{H^{\otimes N}} \frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} (-1)^{a\cdot x} |x\rangle$$

  Thus, we can start with the quantum register $|00\cdots0\rangle$ made of N terms and applying Hadamard we get

$$|00\cdots0\rangle \xrightarrow{H^{\otimes N}} \frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} |x\rangle$$

- Query the oracle - Now applying the function $f_s$ on each qubit, we get the transformation:

$$\frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} |x\rangle \xrightarrow{f_s} \frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} (-1)^{s\cdot x} |x\rangle$$

- Apply Hadamard gates to the input register - since the N hadamard gates is hermitian, we apply this to obtain the secret string s by

$$\frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} (-1)^{s\cdot x} |x\rangle \xrightarrow{H^{\otimes N}} |s\rangle$$

- Measure the first register values and it returns the value of the secret string s directly.

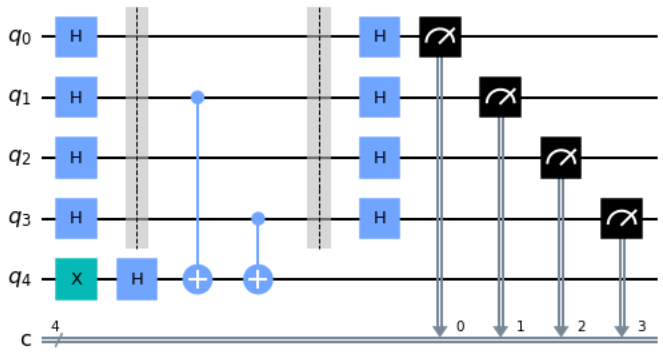



Figure 3.5: Bernstein vazirani algorithm example for 4 qubits

### 3.1.3 Simon's algorithm

[30]

**Value:**

Building on the Bernstein Vazirani algorithm, Simon's algorithm is special as it becomes the foundation for Shor's algorithm and changes the process of searching in a specific way. This was the first quantum algorithm to show an exponential speed-up compared to a classical algorithm, that can be applied to real problems.

**Problem:**

To know if the function is one-one, i.e. if 1 input values relate to 1 output value, or not, and determine the secret string s.

**Classical solution:**

For full certainty, we need atleast $2^{N-1}+1$ computations to know if the function is completely one-one or not. Although there are a few algorithms in classical computing that allows a solution in $\Omega(2^{N/2})$ but the complexity grows exponentially nevertheless.

**Quantum solution:**

- Initialize two N-qubit input registers to the zero state:

$$|\psi_1\rangle = |0\rangle^{\otimes N} |0\rangle^{\otimes N}$$

- Apply a Hadamard transform to the first register:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} |x\rangle |0\rangle^{\otimes N}$$

- Apply the query function $Q_f$:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} |x\rangle |f(x)\rangle$$

- Measure the second register. A certain of $f(x)$ is observed. According to the setup, the observed value correspond to two possible inputs: $x$ and $y = x \oplus b$ which transforms the first register as:

$$\psi_4 = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$$

- Now applying the Hadamard:

$$\psi_5 = \frac{1}{\sqrt{2^{N+1}}} \sum_{z\in\{0,1\}^N} [(-1)^{x\cdot z} + (-1)^{y\cdot z}] |z\rangle$$

- Now, measuring the first register will give an output only if

$$(-1)^{x\cdot z} = (-1)^{y\cdot z}$$

  which gives

$$x \cdot z = (x \oplus b) \cdot z (mod 2)$$

  and after applying $(z_1 \oplus z_2) \cdot z_3 = z_1 \cdot z_2 \oplus z_1 \cdot z_3$, we get

$$x \cdot b = 0$$

- Moreover, as the string $x \in \{0,1\}^n$ is measured, whose inner product with b = 0, thus repeating the algorithm n times we find m different values of x's bit strings such that satisfy $x \cdot b = 0$ from which b can be determined by gaussian elimination. (classical postprocessing)

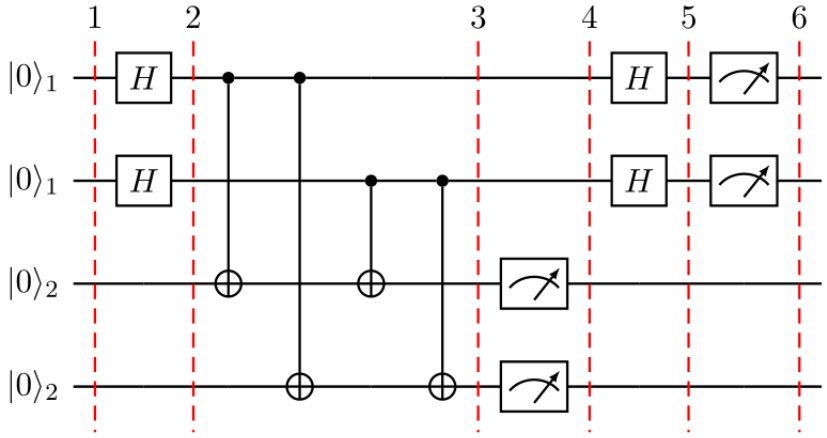



Figure 3.6: Simon's algorithm example

Here, we run Simon's circuit $m = O(n)$ times, instead of exactly n times, since we could potentially measure the same output string, say $x_i = x_j$, at two different runs of the circuit, and we need at least n equations in order to solve the system.

### 3.1.4 Quantum phase estimation algorithm

[33]

**Value:**

It serves as a central building block for many qauntum algorithms and implements a measurement for essentially any Hermitian operator. It is basically defining a different measurement plane for a qubit in quantum computing and is thus subroutine in other algorithms. When a qubit is represented as a vector in 3d space in a Bloch sphere, and this algorithm helps to identify the distinct feature of a qubit - its phase in the imaginary plane. Thus, it only exists for quantum computation and has no classical substitute.

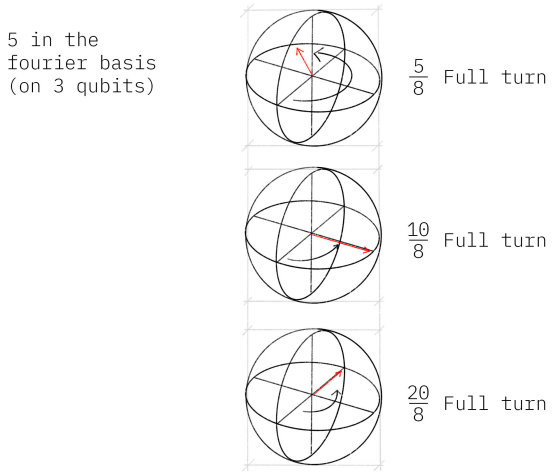



Figure 3.7: Representation of quantum phase algorithm in terms of bloch spheres

**Problem:**

To determine the phase of an eigenvector of a unitary gate given a quantum state proportional to the eigenvector and access to the gate.

**Quantum Solution:**

Here, the use of fourier transforms can help us to find the phase of the qubit easily.

- Setup: $|\psi\rangle$ is in one set of qubit registers. An additional set of N qubits form the counting register on which we will store the value $2^N\theta$:

$$|\psi_0\rangle = |0\rangle^{\otimes N} |\psi\rangle$$

- Superposition: Apply a N-bit Hadamard gate operation $H^{\otimes N}$ on the counting register:

$$|\psi_1\rangle = \frac{1}{2^{N/2}}(|0\rangle + |1\rangle)^{\otimes N} |\psi\rangle$$

- Controlled Unitary Operations: We need to introduce the controlled unitary CU that applies the unitary operator U on the target register only if its corresponding control bit is $|1\rangle$. Since U is a unitary operator with eigenvector $|\psi\rangle$ such that $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$, this means:

$$U^{2^j}|\psi\rangle = U^{2^j-1}U|\psi\rangle = U^{2^j-1}e^{2\pi i\theta}|\psi\rangle = \cdots = e^{2\pi i 2^j\theta}|\psi\rangle$$

  Applying all the N controlled operations $CU^{2^j}$ with $0 \leq j \leq N-1$, and using the relation $|0\rangle \otimes |\psi\rangle + |1\rangle \otimes e^{2\pi i\theta}|\psi\rangle = (|0\rangle + e^{2\pi i\theta}|1\rangle) \otimes |\psi\rangle$, we get

$$|\psi_2\rangle = \frac{1}{2^{N/2}} \sum_{k=0}^{2^N-1} e^{2\pi i\theta k} |k\rangle \otimes |\psi\rangle$$

  where k denotes the integer representation of n-bit binary numbers.

- Inverse Fourier Transform: The QFT maps an N-qubit input state $|x\rangle$ into an output as:

$$QFT|x\rangle = \frac{1}{2^{N/2}}(|0\rangle + e^{\frac{2\pi i}{2}x}|1\rangle) \otimes (|0\rangle + e^{\frac{2\pi i}{2^2}x}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle)$$

Here by using the inverse of this unitary transformation and recovering the state $\left|2^N\theta\right\rangle$ in x, we get

$$|\psi_3\rangle = \frac{1}{2^{N/2}} \sum_{k=0}^{2^N-1} e^{2\pi i\theta k} |k\rangle \otimes |\psi\rangle \xrightarrow{QFT_N^{-1}} \frac{1}{2^N} \sum_{x=0}^{2^N-1} \sum_{k=0}^{2^N-1} e^{-\frac{2\pi ik}{2^N}(x-2^N\theta)} |x\rangle \otimes |\psi\rangle$$

- Measurement: The above expression peaks near $x = 2^N\theta$. For the case when $2^N\theta$ is an integer, measuring in the computational basis gives the phase in the auxiliary register with high probability:

$$|\psi_4\rangle = \left|2^N\theta\right\rangle \otimes |\psi\rangle$$

For the case when $2^N\theta$ is not an integer, it can be shown that the above expression still peaks near $x = 2^N\theta$ with probability better than $4/\pi^2 \approx 40\%$

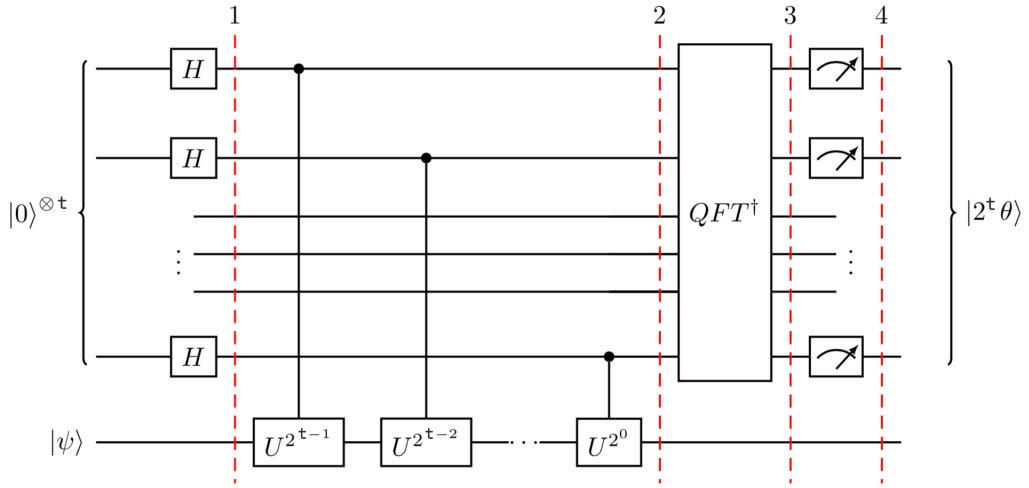



Figure 3.8: Example of quantum phase algorithm

### 3.1.5 Shor's Algorithm

[29]

**Value:**

There has been a problem in quantum cryptography for a long time, i.e. finding the prime factors that when multiplied can be used for encyption purposes. Not even the largest supercomputers can factorize very large numbers. A solution of this problem was proposed by mathematicial Peter Shor in 1994 where the algorithm runs in polynomial time using fast multiplication. It has great applications in internet banking and encryption by integer factorizing the two prime numbers whose multiplication gives us a secret key for encryption.

**Problem:**

To find the two prime numbers that make up a secret key.

**Classical Solution:**

We try to find the distinct prime factors by finding the divisors by selecting all numbers and run the algorithm again and again which is very very troublesome for very large numbers. We can

convert this problem into a period-finding machine. Let N be the product of two distinct prime factors:

$$N = p_1 p_2$$

Now we pick a random integer a between 2 and N-1 to compute the greatest common divisor using Euclid's algorithm (most efficient). If $N$ and $a$ have common prime factors, then we have recieved our answer.

If that's not the case, we can assume that $gcd(N, a) = 1$, so let r be the period of a modulo N and we can take random choices of $a$ until $r$ is even. This gives that $a^r - 1$ is a multiple of N, and $a^{r/2} - 1$ is not. If we assume $a^{r/2} + 1$ is also not a multiple of N, we can find $p_1, p_2$ by simply computing $gcd(N, a^{r/2} \pm 1)$. If $a^{r/2} + 1$ is a multiple of N, we try for another integer of $a$. Thus, we can look at the problem like the periodic function:

$$f(x) = a^x mod N$$

where $a$ and $N$ are the positive integers, $a$ less than $N$ and have no common factors and the period is the smallest integer such that $a^r mod N = 1$. We can solve it classically but it computes for all values of $a$ to find periods, which is computed in exponential times for the outcomes.

**Quantum Solution:**

Shor's solution for this problem uses Simon's algorithm approach with quantum phase estimation.

- First we produce the unitary operator:

  $$U|y\rangle \equiv |aymodN\rangle$$

  Here, we can see that U multiplies the state of our register by $a(modN)$, to get the original state after r appications.

- A superposition of these states in this cycle ($|u_0\rangle$) would be an eigenstate of U:

  $$|u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left| a^k mod N \right\rangle$$

- The above gives the eigenstate with eigenvalue 1, so we take the case where phase is different for each computational basis state, and when the phase of $k^{th}$ state is proportional to k, it gives

  $$|u_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}} \left| a^k mod N \right\rangle$$

  and

  $$U|u_1\rangle = e^{\frac{2\pi i}{r}} |u_1\rangle$$

- Thus, a unique eigenstate for each integer value can be created as $0 \leq s \leq r-1$. By summing all the eigenstates, different phases cancel out, except $|1\rangle$, so we get

  $$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$$

  which means our phase is given by

  $$\phi = \frac{s}{r}$$

  where $s$ is a random integer between 0 and $r - 1$

- Finall, we use the continued fractions algorithm on $\phi$ to find $r$.

Thus, Shor's algorithm is an effective method to compute the prime factors using s and r with exponentially less computations.

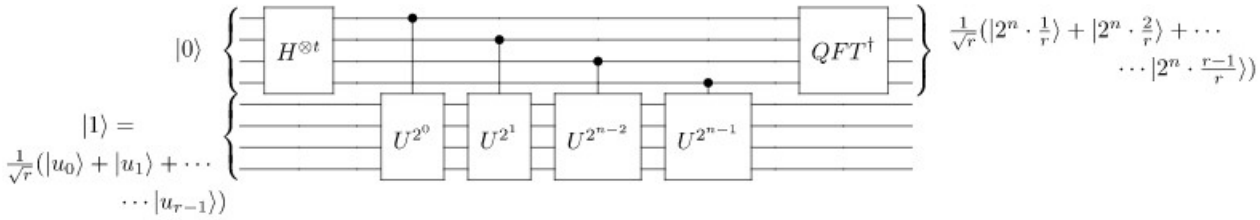



Figure 3.9: General quantum circuit for Shor's algorithm

### 3.1.6 Other Problems

#### Hidden Subgroup problem

[35]

**Value:**

While studying Simon's and Shor's algorithm, we understand the need to generalize the computing problem for other similar problems like discrete logarithms, graph isomorphisms and shortest vector problems. It is basically finding a hidden subgroup in a group which satisfies our desired function requirement. Thus, it has the ability to solve complex problems for finite Abelian (order-independent) groups which is used for Shor's algorithm, discrete logarithm algorithm, solving Pell's equation, etc., while different algorithms for Hidden subgroup problems in case of non-Abelian groups for solving graph isomorphism problem and shortest vector problems.

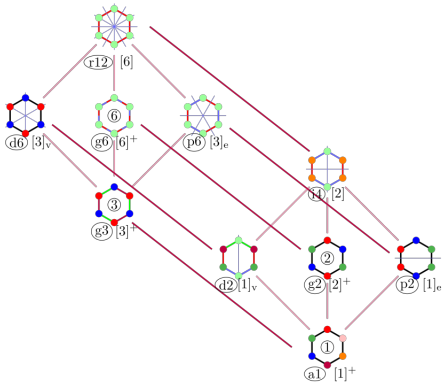



Figure 3.10: Representation of the hidden subgroup problem

**Problem:**

To find a hidden subgroup in finite number of groups - abelian(independent of order) or non-abelian.

Given a known group G and a function $f : G \to S$ where S is some finite set. To find a subgroup $H \leq G$ such that the function f is constant within each coset, and distinct on different cosets: $f(g) = f(g')$ iff $gH = g'H$

**Quantum Solution:**

If G is **Abelian** i.e. the groups are commutative in property (generalizing Shor's algorithm), and function $f : G \to S$ we use HSP as:

- Start with $|0\rangle |0\rangle$, where the two registers have the dimension $|G|$ and $|S|$ respectively.
- Create a uniform superposition over G in the first first register: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle$
- Compute f in superposition: $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$.
- Measure the second register. This yields some value $f(s)$ for unknown $s \in G$. The first register collapses to a superposition over the g in the same f-value as s (i.e., the coset $s + H$): $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |s + H\rangle$
- Apply the QFT corresponding to G to this state, giving $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |\chi_{s+h}\rangle$.
- Measure and output the resulting g.

The key to this algorithm lies in step 5 where it maps the uniform superposition over the coset $s + H$ to a uniform superposition over the labels of set $H^{\perp} = \{\chi_k | \chi_k(h) = 1 for all h \in H\}$,

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |\chi_{s+h}\rangle = \frac{\sqrt{|H|}}{\sqrt{|G|}} \sum_{g : \chi_g \in H/perp} \chi_s(g) |g\rangle$$

For **Non-Abelian** groups, QFTs applied are much more complex than in abelian case since the density matrix $\rho$ has dimension $d > 1$, thus we assume loss of generality and make the unitary matrix using $dim(\rho) X dim(\rho)$ and the corresponding QFT given as:

$$|g\rangle \longmapsto \sum_{\rho \in \hat{G}} \sqrt{\frac{dim(\rho)}{|G|}} |\rho\rangle \sum_{i,j=1}^{dim\rho} \rho(g)_{ij} |i, j\rangle$$

**Boson Sampling problem**

[13]

**Value:**

It is a restricted model of non-universal quantum computation using probability distribution of output dependent on input and unitarity. It is the first step in building a post-classical quantum computer, with a linear optical approach. This task is completely intractable for a classical computer, and a quantum computer approaches it as a photonic version of the bosonic particles itself as it has to be classically potrayed by the permanents of unitary transform matrices of probabilities. We understand that the probability distribution of fermions and bosons is different as evaluating permanence probabilities of bosons is complex. This problem is tackled quantum mechanically as

the bosonic information is imprinted in a photonic form and the photons are sent through glass chips for computation.

**Problem:**

To create a model for probabilistic distribution of bosons with single-photon sources, passive linear optics and photodetection.

**Quantum Solution:**

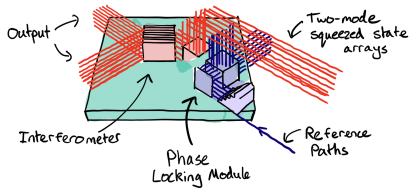



Figure 3.11: Basic setup for boson sampling

- We prepare an input state comprising n single photons in m modes,

$$|\psi_{in}\rangle = |1_1, \cdots, 1_n, 0_{n+1}, \cdots, 0_m\rangle = \hat{a_1}^\dagger \cdots \hat{a_n}^\dagger |0_1, \cdots, 0_m\rangle$$

  where $\hat{a_i}^\dagger$ is the photon creation operator in the $i^{th}$ mode.

- The input state is evolved via a passive linear optics network, which implements a unitary map on the creation operators.

$$\hat{U}\hat{a_i}^\dagger\hat{U}^\dagger = \sum_{j=1}^{m} U_{i,j}\hat{a_j}^\dagger$$

- Any $\hat{U}$ may be efficiently decomposed into $O(m^2)$ optical elements. The output state is a superposition of the different configurations of how the n photons could have arrived in the output modes,

$$|\psi_{out}\rangle = \sum_S \gamma_S \left| n_1^{(S)}, \cdots, n_m^{(S)} \right\rangle$$

  where S is a configuration, $n_i^{(S)}$ is the number of photons in the $i^{th}$ mode associated with configuration S, and $\gamma_S$ is the amplitude associated with configuration S.

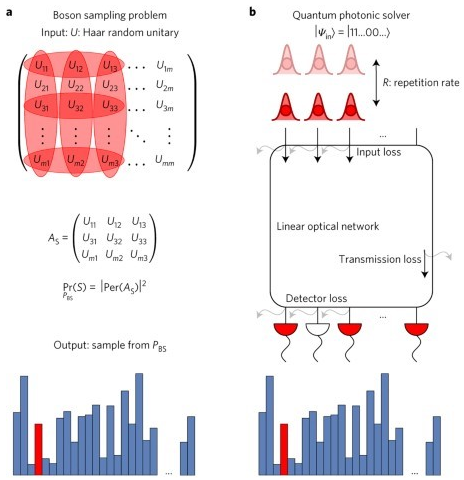



Figure 3.12: Boson sampling quantum circuit

- The probability of measuring configuration S is given by $P_S = |\gamma_S|^2$. where $\gamma_S$ is the amplitude related to matrix permanents given as

$$\gamma_S = \frac{Per(U_S)}{\sqrt{n_1^{(S)}!, \cdots, n_m^{(S)}!}}$$

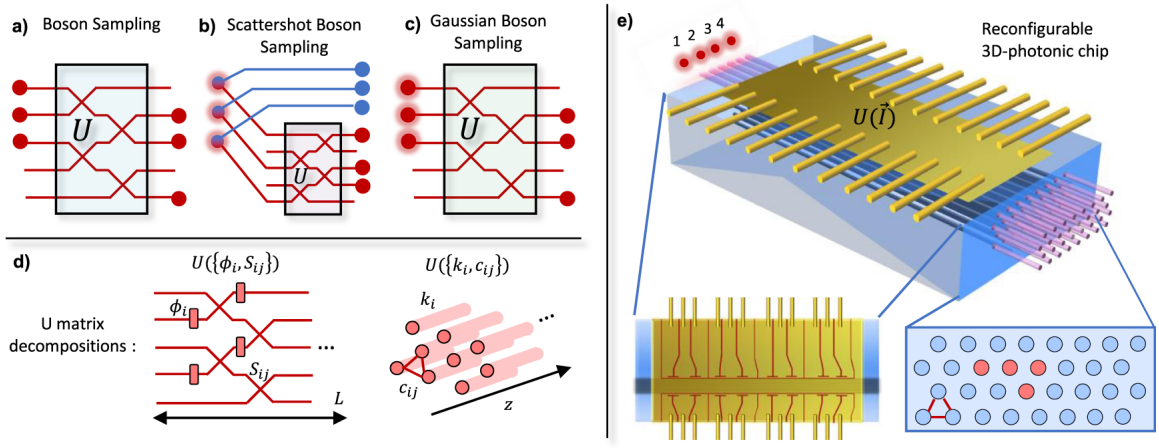



Figure 3.13: Sample circuits for different boson sampling problems

We use linear optical elements to implement non-deterministic quantum computation, probability of success of quantum gates approach unity, and coding methods that achieve fault tolerance.

**Estimating Gauss Sums**

[34]

**Value:**

Gauss sum is a prevalent problem in number theory where we find solutions to summing sequences and are used to prove quadratic reciprocity, cubic reciprocity, quartic reciprocity and calculating the number of solutions of polynomial equations over finite fields, and thus can be used to calculate certain zeta functions. Closely related, these algorithms can be used to find estimation of gauss sums using Jacobi sums.

**Problem:**

To find the Gauss sum for a finite field, i.e. the finite sum of roots of unity.
The Gauss sum of a Dirichlet character modulo N can be represented as

$$G(\chi) = \sum_{a=1}^{N} \chi(a) e^{\frac{2\pi i a}{N}}$$

So, the Gauss sum for a finite ring can be written as the finite versions of the gamma function

$$\Gamma(s) := \int_0^\infty x^{s-1} e^{-x} dx$$

.

**Quantum Solution:**

- Here, let $\zeta_p := e^{2\pi i/p}$ be the $p^{th}$ root of unity, trace of an element x of the finite field $F_{p^r}$ be $Tr(x) := \sum_{j=0}^{r-1} x^{p^j}$ For the finite field $F_{p^r}$, and every multiplicative character written as a function $\chi(x) := \zeta_{p^r-1}^{\alpha \log_g(x)}$, and the additive character $e_\beta$, we can define the Gauss sum G by

$$G(F_{p^r}, \chi, \beta) := \sum_{x \in F_{p^r}} \chi(x) \zeta_p^{Tr(\beta x)}$$

- We apply the quantum Fourier transform over the finite field to the state $|\chi\rangle$, followed by a phase change $|y\rangle \mapsto \chi^2(y) |y\rangle$, thus creating an overall phase change according to

$$|\chi\rangle := \frac{1}{\sqrt{p^r(p^r-1)}} \sum_{y \in F_{p^r}} \chi(x) |x\rangle \longmapsto \frac{G(F_{p^r}, \chi, \beta)}{\sqrt{p^r}} |\chi\rangle$$

- Now estimate the angle $\gamma$ in the equation $G(F_{p^r}, \chi, \beta) = \sqrt{p^r} \cdot e^{i\gamma}$

For any $\epsilon > 0$, there exists a quantum algorithm that estimates the phase $\gamma$ in $G(F_{p^r}, \chi, \beta) = \sqrt{p^r} \cdot e^{i\gamma}$, with estimated error $E[|\gamma - \tilde{\gamma}|] < \epsilon$. The time complexity of this algorithm is bounded by $O(\frac{1}{\epsilon} \cdot polylog(p^r))$

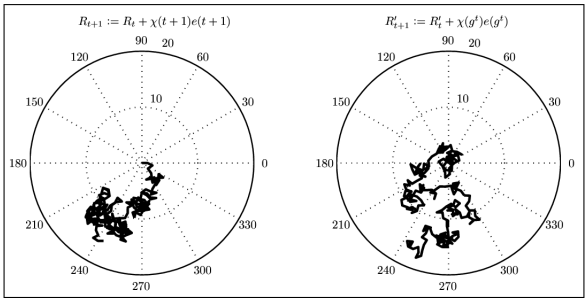



Figure 3.14: Pseudorandom walk for Gauss sum representation

**Fourier Fishing and Fourier Checking**

[1]

**Value:**

These algorithms can create a distinction between classical and quantum computation (i.e. computation for the Fourier transform is really different).

Fourier Fishing - It is the algorithm to to create a fourier transform using the Hadamard- Fourier transform which succeeds with certain probability.

Fourier Checking - Here, once we have built the fourier transform iteself, this algorithm checks for the nature of two functions (independent or forrelated) based on the fourier transforms constructed.

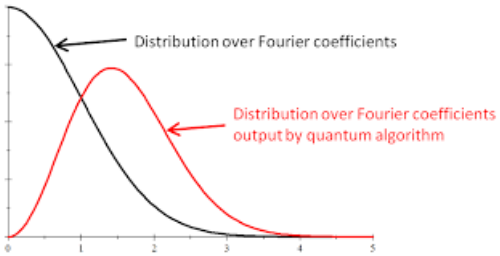



Figure 3.15: Representation of quantum fourier fishing advantage

**Problem:**

Fourier Fishing -

For a given oracle access to n Boolean functions $f_1, \cdots, f_n : \{0,1\}^n \to \{-1,1\}$, we output the strings $z_1, \cdots, z_n \in \{0,1\}^n$ such that atleast 75% times it satisfies $|\hat{f}_i(z_i)| \geq 1$ and atleast 25% times it satisfies $|\hat{f}_i(z_i)| \geq 2$.

Fourier Checking -

Given the boolean functions $f, g : \{0,1\}^n \to \{-1,1\}$, and to check which of the following case it is:

i $\langle f, g \rangle$ is from a uniform distribution $U$ such that every $f(x)$ and $g(y)$ is independent of each other

ii $\langle f, g \rangle$ is from a forrelated distribution $F$ where g is extremely well correlated with f's Fourier transform over $Z_2^n$, i.e. if

$$f(x) := sgn(\alpha) := \begin{cases} 1 & if \alpha \geq 0 \\ -1 & if \alpha < 0 \end{cases}$$

then with Fourier transform

$$g(x) := sgn(\hat{v_x}) := \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} v_x$$

**Quantum Solution:**

Fourier Fishing:

- For n quantum queries, first prepare the state

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} f_i(x) |x\rangle$$

,

- Now apply Hadamard gates to all n qubits
- Now measure in the computational basis and output the result as $z_i$., and the probabilities are given as

$$p_i = \frac{1}{N} \sum_{z_i:|\hat{f}_i|\geq 1} \hat{f}_i(z_i)^2 \text{and} q_i = \frac{1}{N} \sum_{z_i:|\hat{f}_i|\geq 2} \hat{f}_i(z_i)^2$$

It succeeds with probability $1 - \frac{1}{e^n}$, where the probability is over both $\langle f_1, \cdots, f_n \rangle$ and the algorithm's internal randomness.

Fourier Checking:

- Prepare a uniform superposition over all $x \in \{0,1\}^n$ and query f, we create the state

$$\frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} f_i(x) |x\rangle$$

- Apply Hadamard gates to all n qubits to create the state

$$\frac{1}{N} \sum_{x,y\in\{0,1\}^n} f(x)(-1)^{x\cdot y} |y\rangle$$

- Now query g in superposition to create the state

$$\frac{1}{N} \sum_{x,y\in\{0,1\}^n} f(x)(-1)^{x\cdot y} g(y) |y\rangle$$

- Apply Hadamard gates to all n qubits again, to create the state

$$\frac{1}{N^{3/2}} \sum_{x,y\in\{0,1\}^n} f(x)(-1)^{x\cdot y} g(y)(-1)^{y\cdot z} |z\rangle$$

- Finally measure in the computational basis, and "accept" if and only if the outcome $|0\rangle^{\otimes n}$ is observed. If needed, repeat the whole algorithm $O(1)$ times to boost the success probability.

It is clear that the probability of observing $|0\rangle^{\otimes n}$ (in a single run of FC-ALG) equals

$$p(f,g) := \frac{1}{N^3} ( \sum_{x,y\in\{0,1\}^n} f(x)(-1)^{x\cdot y} g(y))^2$$

It is a problem of deciding whether $p(f,g) \geq 0.05$ or $p(f,g) \leq 0.01$, promised that one of these is the case. Thus, we immediately get a quantum algorithm to solve it with constant error probability using $O(1)$ queries to find f and g.

## 3.2 Based on amplitude ampification - BQP

Quantum computing also allows us to use amplification of an amplitude of a quantum state in order to find solutions. This is another method of altering the quantum state, opening up a different range of problems for quantum computations, especially in case of unstructured search algorithms.

Here, the chosen subspace of a quantum state is allowed to be applified which leads to quadratic speedups over the corresponding classical algorithms. In a visual sense, we can imagine it in a way where we add to the subspace of a Bloch sphere of a quantum vector to find solutions, i.e. we rotate the vector space in its reflection to find the solutions(which has a negative phase). Since we are dealing with amplitudes of the qubit directly in this case and not probabilities, we can find solutions in $\sqrt{N}$ queries.

### 3.2.1 Grover's algorithm

[21]

**Value:**

Searching is one of the most important algorithms and a quantum computer has the potential for superior speed searching algorithms, especially in the case of unstructured lists.

**Problem:**

To search for a marked entry in an unstructured list of N entries.

**Classical Solution:**

There are many algorithms in classical computing like linear search, binary search, jump search, etc. by sorting the data and then efficiently searching through the ordered list.

With these search techniques, they increase the computation power by reducing number of measurement checks, and the optimum average of these running checks come out to N/2 queries and in worst case, N queries.

**Quantum solution:**

Here, we find that a quantum approach can give the result through an oracle which is computed in $\sqrt{N}$ queries rather than N queries.

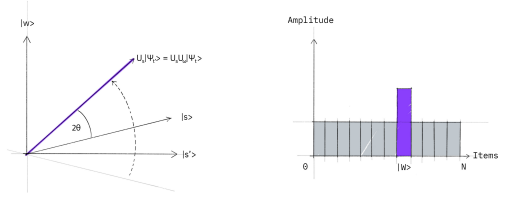



Figure 3.16: Representation of the grover's algorithm

Here, the grover's algorithm solves the problem by adding a negative phase to the solution states, i.e. for any state $|x\rangle$ and a searchable item w in the computational basis:

$$U_w |x\rangle = \begin{cases} |x\rangle & \text{if} x \neq w \\ -|x\rangle & \text{if} x = w \end{cases}$$

The oracle is just an identity matrix with one little modification: negative phase for the item to be searched.

- The amplitude amplification procedure starts out in the uniform superposition $|s\rangle$, which is easily constructed from $|s\rangle = H^{\otimes n} |0\rangle^N$
- We apply the oracle reflection $U_f$ to the state $|s\rangle$.
- We now apply an additional reflection($U_s$) about the state $|s\rangle : U_s - 2|s\rangle\langle s| - 1$.
- We repeat the previous steps, i.e. applying the oracle reflection and rotation and we need roughly $\sqrt{N}$ rotations to find the item in the unstructered list.

Note: Since we are dealing with amplitudes and not probabilities, the vector space's dimension enters as a square root. Thus, it is the amplitude and not just probability that is amplified.

The procedure stretches out or amplifies the amplitude of the marked item, which shrinks the other items' amplitude, so that measuring the final state will return the right item with near certainty.

Here, we use two reflections generating rotations in a two-dimensional plane - winner $|w\rangle$ and uniform superposition $|s\rangle$ (Note: these are not quite perpendicular since $|w\rangle$ occurs in the superposition with $\sqrt{N}$ amplitude), and an additional state $|s'\rangle$ is made as a perpendicular to $|w\rangle$ so that $|s\rangle$ can be represented in $|s'\rangle$ and $|w\rangle$ plane.

Also, in case of multiple M solutions, $\sqrt{(N/M)}$ rotations can result in a solution.

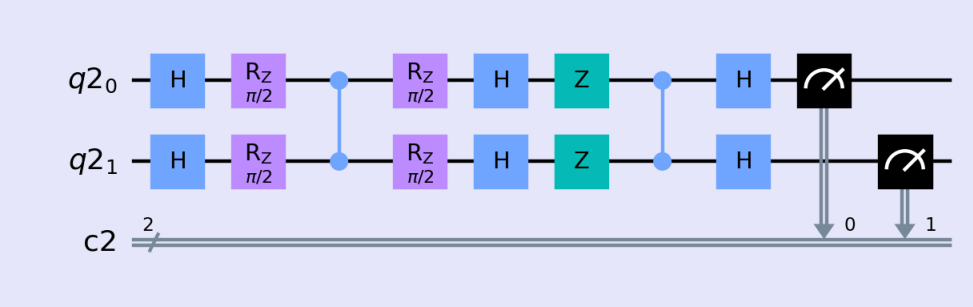



Figure 3.17: Grover's algorithm application for 2 qubits

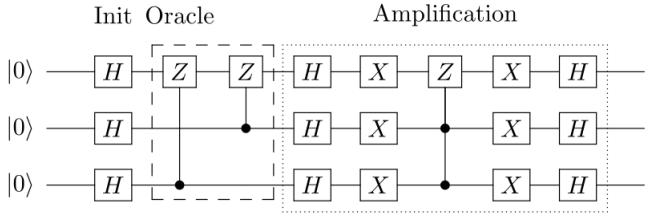



Figure 3.18: Grover's algorithm application for 3 qubits

### 3.2.2 Quantum Counting

[5]

**Value:**

This is basically a generalization of the search problem. This is based on the quantum phase estimation algorithm and grover's search algorithm.

**Problem:**

To count the number of marked entries in an unordered list(not detecting)

**Classical solution:**

We perform N computations to determine the number of solutions in the N elements of the list.

**Quantum solution:**

Here, we simply use the quantum phase estimation algorithm to find the eigenvalue of a grover search iteration. It rotates the state vector by $\theta$ in the $|w\rangle, |s'\rangle$ basis. The eigenvalues of the Grover iterator are $e^{\pm i\theta}$ which can be extracted to find the number of solutions.

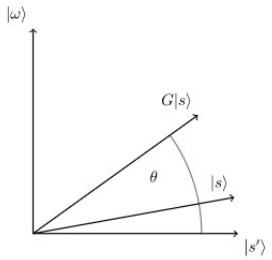



Figure 3.19: Qauntum counting representation

In the $|w\rangle, |s'\rangle$ basis we can write the Grover iterator as the matrix:

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

The matrix G has eigenvectors:

$$\begin{pmatrix} -i \\ 1 \end{pmatrix}, \begin{pmatrix} i \\ 1 \end{pmatrix}$$

With the eigenvalues $e^{\pm i\theta}$, and a state $|s\rangle$ is a superposition given as:

$$|s\rangle = \alpha |w\rangle + \beta |k'\rangle$$

Thus, we measure the register to obtain one of these two values and use simple maths to get our estimate of M number of solutions.

## 3.3 Based on quantum walks - BQP

Here, quantum property of probability distribution is used for computing purposes. It is a quantum analogue to a classical random walk, and is based on a probability distribution over some states which is achieved through quantum superposition over the quantum states. They provide exponential speedups for some problems, and polynomial speedups for some other problems. Here, we try to solve real problems that are very hard in classical computing by relating the problem statement directly to the qubit states and the corresponding probability function is calculated.

Quantum walks can be related to decision trees to evaluate a problem, i.e. every problem is subdivided into many different components along a path of a decision tree and every path is

correspondent to a specific probability distribution, which returns us the solution for our concerned problem.

We would take an analogy to classical random walks and then build towards a general quantum walk which can then be optimized to a specific problem. In classical walks, we can have a discrete-time random walk or a contunous-time random walk, where continuous-time walk can performed either by generating a pseudo-random number at each step according to which particle's position is updated in the walk map, or by having an array representing probabilities of each position stored and updated via a stochastic matrix which determines the time evolution of the system.

Taking inspiration from this, a quantum walk can be discrete where a coin register states the particle's position and a position register tracks the probability distribution of the particle at a particular position, or continuous where we convert the exponential behaviour of a classical to oscillatory behaviour using quantum states as they are based on probability distributions.

We can observe that while classical walks are symmetrical, quantum walks have constructive and destructive interference of amplitudes(can be make symmetrical with specific initial conditions). Also, to check for the speed of the spread of quantum walks, we can compare the variances, i.e. classical variance is $\sigma_C^2 = T$ after T steps, but quantum variance is $\sigma_Q^2 = T^2$ after T steps, thus exponentially faster propagational factor.

### 3.3.1 Element distinctness problem

[26]

**Value:**

While studying the collected information, there is a need to understand the distinctness of all the elements which can dictate the problem's complexity. We understand that a problem's time complexity is an oracle on $n \log n$, i.e. both the upper and lower bounds for time complexity is in a linearithmic scale. This can also be generalized for finding elements that occur more than once according to N/k times with a list of N entries, and k as the no of repetitions.

**Problem:**

To determine whether all elements in the list are distinct.

**Classical solution:**

Here, an algebraic computation tree model can be constructed and computation works in a polynomial time classically. There are different approaches to achieving this and the most prevalent among these are:

- The list is sorted first and then checked for consecutive equal elements.
- Solved in linear expected time using randomized algorithm that inserts each item into a hash table and compares elements of the the same hash table cell.
- Solved through an asymptotically optimum algorithm of linearithmic time complexity

**Quantum solution:**

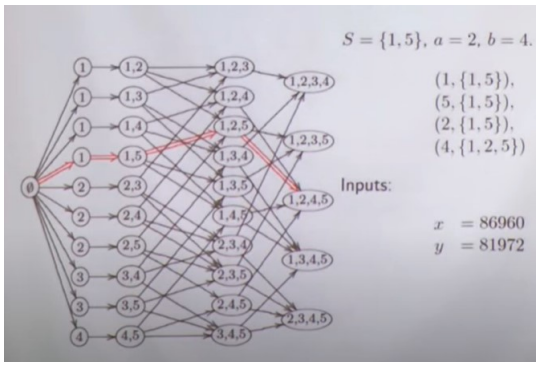



Figure 3.20: Representation of element distinctness algorithm

The problem's time complexity is given as an oracle for $n \log n$ and the problem is accessed by computing and comparing simple algebraic functions of the values of the hash tables. the lower bound for solving these problems is $N^{2/3}$ queries instead of N queries as in classical solution. This is done through the decision tree model of computation.

The algorithm uses two registers. A vector of the computation basis has the form

$$|S, y\rangle \otimes \left|x'_1, \cdots, x'_{r+1}\right\rangle$$

The Hilbert space has dimension $\binom{N}{r}(N-r)M^{r+1}$ and the memory in qubits is then $O(r(\log_2 N + \log_2 M))$

The initial state is

$$\frac{1}{\sqrt{\binom{N}{r}(N-r)}} \sum_{(S, y \in \nu)} |S, y\rangle |0, \cdots, 0\rangle$$

The first step is to query each $x_i$ for $i \in S$ and with $S = \{i_1, \cdots, i_r\}$ the next state is

$$\frac{1}{\sqrt{\binom{N}{r}(N-r)}} \sum_{(S, y \in \nu)} |S, y\rangle |x_i, \cdots, x_{i_r}, 0\rangle$$

Main block:

1. Repeat this step the following number of times: $t_1 = \lfloor \frac{\pi}{4}\sqrt{r} \rceil$

(a) Apply a conditional phase-flip operator R that inverts the phase of $|S, y\rangle \left|x'_1, \cdots, x'_{r+1}\right\rangle$ if and only if there is a k-collision for distinct indices $K = \{i_1, \cdots, i_k\}$ in S, that is,

$$R\,|S, y\rangle\, x'_1, \cdots, x'_{r+1} = \begin{cases} -\,|S, y\rangle \left|x'_1, \cdots, x'_{r+1}\right\rangle, & \text{k-collision for} K \subseteq S \\ |S, y\rangle \left|x'_1, \cdots, x'_{r+1}\right\rangle, & \text{otherwise} \end{cases}$$

(b) Repeat the Subroutine the following number of times: $t_2 = \lfloor \frac{\pi\sqrt{r}}{2\sqrt{k}} \rceil$.

2. Measure the first register and check whether S has a k-collision using a classical algorithm.

Subroutine:

1. Apply operator $U_\alpha = 2\sum_{S \in S_r} |\alpha_S\rangle\langle\alpha_S| - I$ on the first register.
2. Apply oracle O defined by

$$O\,|S, y\rangle \left|x'_1, \cdots, x'_{r+1}\right\rangle = |S, y\rangle \left|x'_1, \cdots, x'_{r+1} \oplus x_y\right\rangle$$

, which queries element $x_y$ and adds $x_y$ to $x'_{r+1}$ in the last slot of the second register.
3. Apply operator $U_\beta^{EXT}$, defined by

$$U_\beta^{EXT} = 2 \sum_{x'_1,\cdots,x'_{r+1}} \sum_{[S,y]\in\nu/\sim} \left|\beta_{[S,y]}^{x'_1,\cdots,x'_{r+1}}\right\rangle\left\langle\beta_{[S,y]}^{x'_1,\cdots,x'_{r+1}}\right| - I$$

, where

$$\left|\beta_{[S,y]}^{x'_1,\cdots,x'_{r+1}}\right\rangle = \frac{1}{\sqrt{r+1}} \sum_{y'\in S\bigcup\{y\}} \left|S\bigcup\{y\}\ \{y'\}, y'\right\rangle \left|\pi(x'_1),\cdots,\pi(x'_{r+1})\right\rangle$$

where $\pi$ is a permutation of the slots of the second register induced by a permutation of the indices of the first register.
4. Apply oracle O.

The total number of quantum queries is $r + \pi^2 r/(4\sqrt{k})$ approximately considering the initial setup and main block. After the measurement, r classical queries are necessary.

Also, the values $t_1 = \frac{\pi}{4}\sqrt{r}$ and $t_2 = \frac{\pi\sqrt{r}}{2\sqrt{k}}$ are asymptotically optimal and the success probability of the algorithm is given as $1 - O(1/r^{1/k})$.

Moreover, we learn that an algorithm which takes N queries classically can be solved in $N^{2/3}$ queries with a quantum computer.

### 3.3.2 Triangle-finding problem

[22]

**Value:**

This problem is a prevalent problem in graph theory based on Hamiltonian closed paths where we find that a graph contains a triangle or not. It is a very complex problem and there is no direct classical algorithm for solving this problem and thus each possible path for a graph is checked classically, which increases in complexity with the increase of nodes.

**Problem:**

Problem: To determine whether a given graph contains a triangle

**Classical Solution:**

Making a 2d variable matrix for each vertex and checking for its neighbour relations. It takes N queries(permutations independent of order).

**Quantum Solution:**

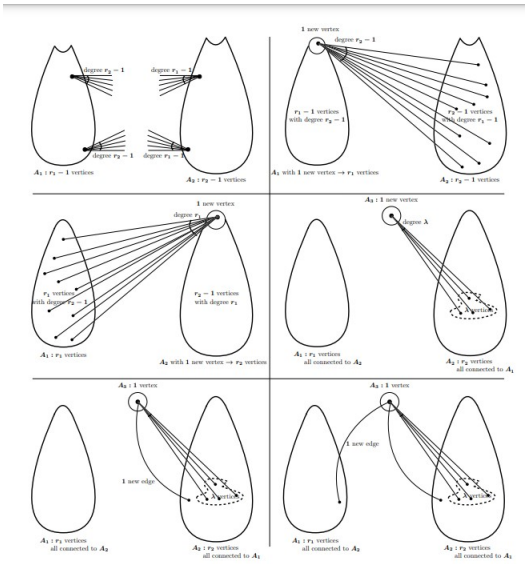



Figure 3.21: Triangle finding representation

Let $G = (V, E)$ denote the undirected and unweighted graph that is the input of the triangle finding problem, and write $n = |V|$. For any vertex $u \in V$, we denote

$$N_G(u) = \{v \in V | \{u, v\} \in E\}$$

the set of neighbors of u.

The algorithm first takes a set $X \subseteq V$ consisting of $\Theta(\sqrt{n} \log n)$ vertices chosen uniformly at random from V, and checks if there exists a triangle of G with a vertex in X. This can be checked, with high probability, using Grover's quantum search in

$$O(\sqrt{|X| * |\epsilon(V)|}) = \tilde{O}(n^{5/4})$$

queries

1. Search for a set $A \subseteq V$ of size $\lceil n^{3/4} \rceil$ such that $(U_{w \in V} \Delta_G(X, A, w)) \cap E \neq \emptyset$, while concurrently constructing $\epsilon(A)/S$, using a quantum walk

2. Search for a vertex $w \in V$ such that $\Delta_G(X, A, w) \cap E \neq \emptyset$

3. Search for a set $B \subseteq A$ of size $\lceil \sqrt{n} \rceil$ such that $\Delta_G(X, A, w) \cap E \neq \emptyset$, while concurrently constructing $\Delta_G(X, B, w)$, using a quantum walk and the fact that $\epsilon(A)/S$ has already been constructed

4. Check if $\Delta_G(X, B, w) \cap E \neq \emptyset$ in $O(n^{1/4})$ queries, using the fact that $\Delta_G(X, B, w)$ has already been constructed.

So basically we define the set $\Delta_G(X, Y, w) \subseteq \Delta_G(X, Y)$ as:

$$\Delta_G(X, Y, w) = \epsilon(Y \cap N_G(w))/ \bigcup_{n \in X} \epsilon(N_G(u)) = \{\{u, v\} \in \Delta_G(X, Y) | \{u, w\} \in E and \{v, w\} \in E\}$$

Also, the query complexity to gaurantee a result can be shown to be $O(n^{5/4})$ (the upper bound for an unweighted graph).

### 3.3.3 Formula Evaluation

[3]

**Value:**

A decision tree can be an effectective way to evaluate a formula with a gate at each internal node, input bit at each leaf node, and the output being the root node which is measured. Thus, we convert the equations into a decision tree and work it in a vertex form (matrix), to evaluate the formula. This can be achieved either through brute force algorithms or by using a random walk, i.e. evaluating the formula through a walk distribution map and the path defined by respective probabilities.

**Problem:**

To evaluate the respective values of a formula i.e. evaluate the balanced binary AND-OR tree with n leaves.

**Classical solution:**

We use NAND, AND, OR gates to evaluate the fomula but it has to travel through all possible configurations to give us the output. A classical decision tree constructed is travelled along a path based on element at a node and its probability.

One effective way is to replace the AND and OR gates with NAND gates to make a full binary tree with NAND gates. Then, this binary tree can be evaluated according to the optimal path for a function taking into account the probablities of each node. We found that an optimum solution of a balanced binary tree with NAND gates would require $N^{0.754}$ queries.

**Quantum solution:**

With the algorithms that we have studied so far, we can solve it by applying grover search in a matrix form to evaluate the highest probable configuration which would require $N^{0.5}$ quantum queries.

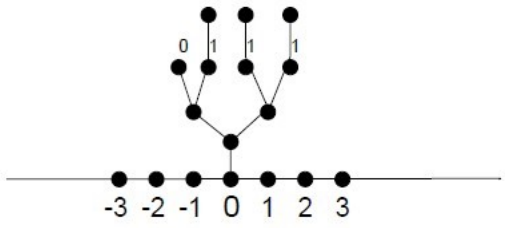



Figure 3.22: Approach to formula evaluation with an augmented tree

However, we strive to achieve more optimal methods for evaluating a formula using a quantum random walk. So, to evaluate the Boolean formula, we create a boolean tree with the variables at the leaves and NAND gates at the internal vertices.

For a continuous time quantum algorithms, we have an infinite line of vertices $x$ connected to vertices $x-1$ and $x+1$ with a certain depth and connecting the root $r$ of our NAND tree to the vertex 0.

Thus, we can create the state as a superposition of the energy eigenstates of H with an energy $E = 2\theta$ as:

$$|\psi_E\rangle = \sum_{n \in Z} \alpha_n |n\rangle + \sum_{v \in T} \alpha_v |v\rangle$$

where $|n\rangle$ are the vertices on the infinite line and $|v\rangle$ are the vertices in the tree. Also the amplitude of the vertices can be shown as:

$$\alpha_n = \begin{cases} e^{i\theta n} + R(E)e^{-i\theta n} & if n < 0 \\ T(E)e^{i\theta n} & if n \geq 0 \end{cases}$$

where $R(E)$ and $T(E)$ are the refelection and transmission coefficients(amplitudes of possibilities of the walk) which depend on the energy E and the structure of the tree.

The starting state can be described as

$$\left|\psi'_{start}\right\rangle = \frac{1}{\sqrt{L+1}} \sum_{k=0}^{L} (-1)^k \left|2k\right\rangle$$

where $L = O(\sqrt{N})$ Here $|0\rangle$ denotes the root of the tree and $|1\rangle \cdots |2L\rangle$ denote the vertices in the tail. Now, evaluating the function, we get If F = 0, then there exists $|\psi\rangle$ such that $H|\psi\rangle = 0$ and $\langle\psi|\psi'_{start}\rangle \geq 1 - \epsilon$ If F=1, then for any eigenstate $|\psi\rangle$ of Hamiltonian H, either the corresponding eigenstate $\lambda$ satisfies $|\lambda| = \Omega(\frac{1}{\sqrt{N}})$ or $|\psi\rangle \perp |\psi_{start}\rangle$

So if F=0, we find one of the basis states $|2k\rangle$ with a high probability and if F=1, we find one of the basis states $|v\rangle$ in the tree.

The continuous time Hamiltonian H can be written as $H = H_{tree} + H_{input}$ where $H_{tree}$ is independent of the variables and $H_{input}$ consists of the extra edges that are added to the tree if any variable is 1.

### 3.3.4 Group commutativity

[22]

**Value:**

With applications of search problems according to structured, unstructured or partially structured databases, we need to determine the query complexity in terms of commutable nature of the query structure. This algorithm is pretty similar to element distinctness problem, as the aim of the former is to check for distinctness of elements i.e. the non-commutativity of the intial and resultant element.

**Problem:**

To determine if a black box group is commutative specified by k generators, i.e. the result is independent of the order of the inputs applied to the black box.

Oracle: Group operations $O_G$ and $O_G^{-1}$ for an encoding in $\{0,1\}^n$ Input: The value of n and the encoding of generators $g_1, \cdots, g_k$ of G Output: Yes if G is commutative, and No otherwise (if there are two indices i,j such that $g_i g_j \neq g_j g_i$)

**Classical Solution:**

Since the application of generators is random, the straightforward algorithm has a complexity $O(k^2)$ where there is a check for commutability of every pair of generators. Even still, Pak showed a classical randomized algorithm whose complexity is linear in k, with a quadratic deterministic lower bound.

**Quantum Solution:**

One way to approach this problem can be solved by using Szegedy quantum walks. By analyzing a simple recurrence, one can show that this algorithm uses:

$$O((\frac{d-1+\sqrt{d^2+14d+1}}{4})^k) = O(n^{\log_d \frac{d-1+\sqrt{d^2+14d+1}}{4}})$$

where $n = d^k$ is the input size.

Szegedy quantum walk :-

Let P be an ergodic and symmetric Markov chain on a graph $G = (V, E)$ on N vertices. We denote by $P[u, v]$ the transition probability from u to v. Let M be a set of marked nodes of V. Assume, one is given a database D that associates some data D(v) to every node $v \in V$. From D(v) we would like to determine if $v \in M$.

Initializing time I: The time complexity for constructing the superposition

$$\frac{1}{\sqrt{N}} \sum_{u,v} \sqrt{P[u, v]} \, |u, v\rangle$$

. Transition time T: The time complexity of realizing the transformation

$$|u, v\rangle \mapsto 2\sqrt{P[u, v]} \sum_{v'} \sqrt{P[u, v']} \, |u, v'\rangle - |u, v\rangle$$

The random walk on $S_l$ is defined simply:

Suppose the current state is $u \in S_l$. With probability 1/2 stay at u; with probability 1/2, do the following:

- pick a uniformly random position $i \in \{1, \cdots, l\}$, and a uniformly random index $j \in \{1, \cdots, k\}$.
- if $j = u_m$ for some m, then exchange $u_i$ and $u_m$, else set $u_i = j$.
- update the tree $t_u$ (using $O(\log l)$ group operations)

With the most optimal method for quantum walk, the oracle is found to be $k^{2/3} \log k$ computations.

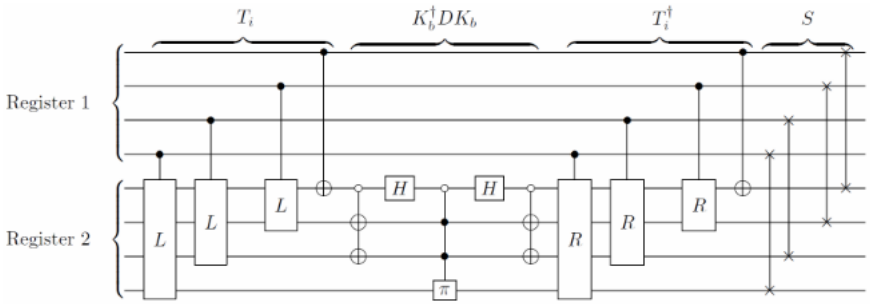



Figure 3.23: Representation of a Szegedy quantum walk on a cyclic path

## 3.4 BQP-complete problems

These are the problems that can be completely solved in a definite polynomial time by a quantum computer. Since these problems take much more exponential time by a classical computer, it would take a very long time for even the fastest classical computers but can be solved in quantum polynomial time. These deterministic problems are one of the practical problems that give a measurable superiority to quantum computers.

### 3.4.1 Computing Knot Invariants

[14]

**Value:**

Just like triangle finding problem, this is one of the most influential computing problems in graph theory. It is based on the knot theory and the goal is to identify a knot invariant or a knot group which is combinatorially identical. The knot theory uses algebraic and geometric techniques to study topological objects which can be represented in different renditions of knots. We can classify the different knots by a number of folds of a knot and we try to find the invariants of a particular knot.

Mathematically, Knot types are classified by the number of folds like 0(unknot), 3(trefoil knot), 4(figure-eight knot) and 6(Stevedore's knot), and their standard knot invariants include the fundamental group of the knot complements, numerical knot invariants(such as Vassiliev invariants), polynomial invariants (knot polynomials such as the Alexander polynomial, Jones polynomial, Kauffman polynomial F, and Kauffman polynomial X), and torsion invariants (such as the torsion number).

**Problem:**

To find if the group members are knot invariants of each other computationally.

**Quantum Solution:**

It is interesting that the isotopy class of a knot diagram can be represented by a matrix relating to each element of a group. This conversion into our solvable problem is done throught the braid notation creating a connection between knots and links.

We apply the basic techniques discussed earlier which describe the way the quantum computers work and modify them to perform the knotted graph group algorithm for computing the knotted graph group in 3 different ways:

- In a given graph $K \subset R^3$, idetify all non-essential vertices that can be removed keeping the isotopy class of K after computing only 3-by-3 determinants.
- For a simplified graph $K' \subset R^3$, find all crossings in a plane diagram of K'. Going along K', compute the Gauss code using the found crossings in the plane diagram of K'. Apply the Reidemeister move R1 for a further reduction if possible.
- Turn a Gauss code into a presentation of the fundamental group $\pi_1(R^3 - K)$ whose abelian invariants can be calculated using efficient algorithms of GAP.

Topological Quantum computers give a more elegant solution to these kind of problems. It can be represented according to the Chern-Simons topological quantum field theory in terms of Jones polynomials which approximates the value efficiently as compared to classical computing.

These topological quantum computers are discussed later in this paper in more detail. In general, we exchange the positions of anyons in space to perform computation. Hence, the swapping of adjacent anyons traces out the plane braids in 2+1 spacetime and the exchange of anyons correspond to a crossing paving way for application of a unitary operator. Moreover, a topological quantum computation is solely dependent on the topology of the braid and is free from local perturbations of the system.

Measurement - After the computation, we can fuse the anyon states to determine the classical result, and the string of fused qubits is the result of the computations. It is interesting that the probability computation formula for returning the all 0 string is equivalent to the Jones polynomial of knot which is the particular kind of closure of this braid. This principle can be used practically in computing the homflypt polynomial where a classical finite type computation is carried out by

vertigan's algorithm while coloured Jones polynomials compute the quantum circuit in $\sqrt{N}$ entries and the dependency on just the geometry of quantum processors makes our tasks much easier, paving way for solving Turaev-Viro invariants of 3-dimensional manifolds too.

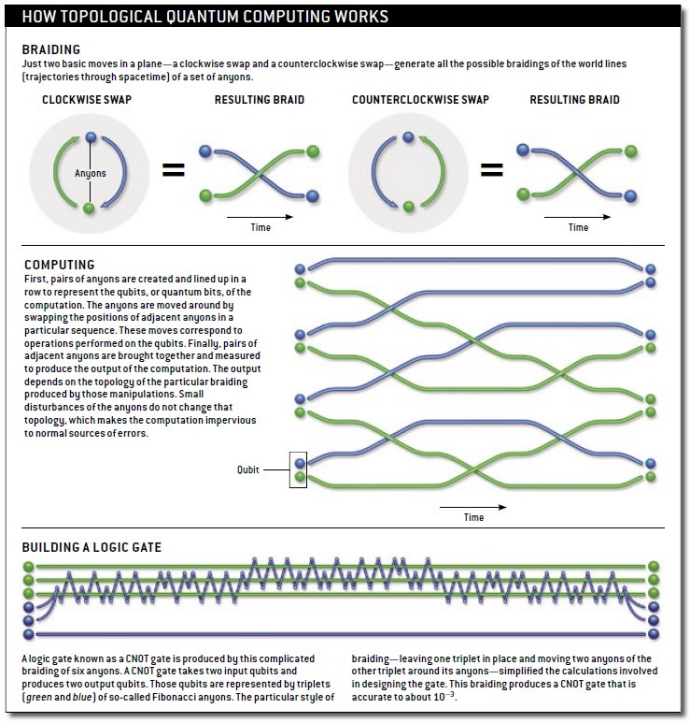



Figure 3.24: Representation of computing knot invariants

### 3.4.2 Quantum Simulations

[7]

**Value:**

In 1981, Richard Feynman said "Nature isn't classical, dammit, and if you want a simulation of nature, you'd better make it quantum mechanical" and since then, we look into the prospects of simulating many-particle quantum systems through quantum computers.

With applications in Quantum Chemistry, Quantum field theory and High energy physics, quantum simulators can help in semi-definite programming, differential equations and simulating quantum systems. These systems revolve along the simulation of the Hamiltonian in order to find our desired result, be it the lowest eigenvalue or finding the coefficients of quantum dynamics. They have many applications including simulating Bosonic and Fermionic systems, geological systems, chemistry problems, and financial models and different approaches are built according to the type of problems. These type of algorithms pave way for different type of quantum computers like topological computers for efficient computation.

**Problem:**

To compile the unitary evolution of a quantum state into a polynomial-sized gate sequence for simulating the Hamiltonian of the system.

**Quantum Solution:**

Here, our aim is to compile the unitary transformation of a physical state to a polynomial sized

gate sequence for a quantum computer. Since we understand that brute force synthesis is unlikely to succeed. our central strategy is to reduce the problem into subproblems that are easy to compile, and thus we can also describe them in 4 broad strategies:

- Trotter-Suzuki formulas

  Here, we break the simulation problem into a sequence of easy problems. Thus, we simulate the exponential function $e^{-iHt}$ by rapidly switching the terms on and off and it behaves like all the terms are on at once and we can convert the function as

  $$e^{-iHt} = (\prod_{j=1}^{m} e^{-\frac{iH_j t}{r}})^r + O(\sum_{j,k} |[H_j, H_k]|t^2/r)$$

  where we have divided the problem into r steps. We compute these problems by transforming the problem into steps of simple transformations connected together to form a resultant desired matrix.
  Example: Pauli-Hamiltonian problem consists of same 2x2 blocks simplifying the circuit.

- Randomized evolution (qdrift, density matrix, exponentiation)

  Here, this type of computation is basically converting our complex problem into creating an easier type of structure that can computed easily. In more detail, we are basically compiling the problem with additional data to convert the respective problem into computable terms and then find a particular solution according to the respective problem.

- Linear combination of unitaries

  Here, we implement a sum of unitary matrices to find the solution. We understand that the sum of unitary matrices is not necessarily unitary, which prevents us to do a classical computation. But in a quantum solution, the idea is to block-encode the sum in a larger unitary, i.e. the sum of unitaries will be a part of the larger unitary and then it can implemented in a quantum circuit. We can then manipulate the computation for highest probability in our desired result to find the solution to our problem.

  Two of the common implementations can be found in Monte Carlo Analogue and Truncated Dyson series. Moreover, this is a great way to simulate a time-independent Hamiltonian by transformations according to an interaction frame.

- Qubitization (quantum walks)

  Here, our principle of quantum computation is basically by building a simple walk operator that is equivalent to our desired function. We can use the oracles in the LCU to build a quantum walk where we build the network into unitary and Hermitian functions and then using Grover's search for the best outcome. So basically, we find a solution by forming a pair of reflections.

  Qubitization is generally implemented for problems in chemistry since they have no self-evident symmetry which can be used as an advantage.

We also understand that the type of simulation depends on the type of problem and we can use some basic grounds for differentiating between these approaches.

**Trotter Suzuki Simulations**

$$\text{Cost} \sim \frac{(\alpha_{comm} t)^{1+\frac{1}{2k}}}{\epsilon^{\frac{1}{2k}}}$$
$$\alpha_{comm} = max_{i,N} |[H_{i_2}]|$$

Pro: Cost scales with commutator of terms and Works for time-dependent H

Con: Not optimal scaling with t or error

**LCU Simulations**

$$\text{Cost} \sim \frac{(\sum_j |\alpha_j| t) \log(\frac{1}{\epsilon})}{\log\log(\frac{1}{\epsilon})}$$

Pro: Very flexible
Works for time-dependent H

Con: empirically more costly
Many ancillae needed

**Qubitization Simulations**

$$\text{Cost} \sim (\sum_j |\alpha_j| t) + \frac{\log(\frac{1}{\epsilon})}{\log\log(\frac{1}{\epsilon})}$$

Pro: Optimal Scaling

Con: Many ancillae needed
Does not work for time-dependent H

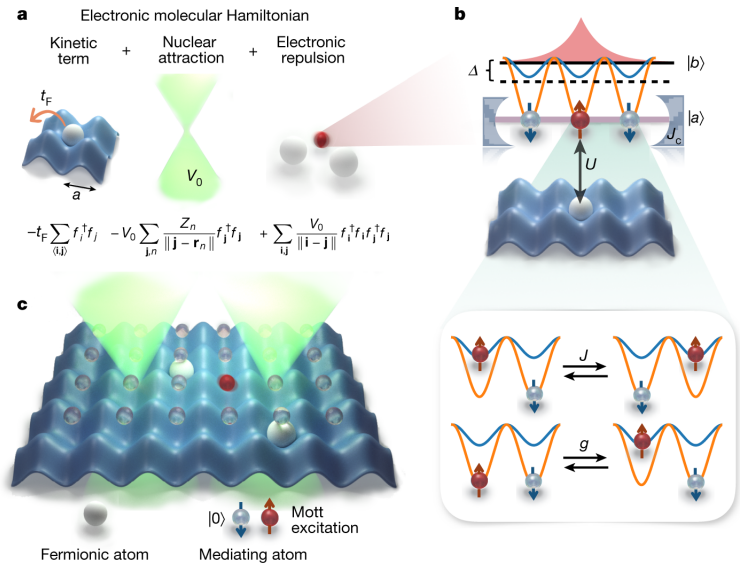



Figure 3.25: Example of an analogue quantum chemistry simulation

### 3.4.3 Solving a linear system of equations

[15]

**Value:**

We know that linear system of equations are uqiquitous in engineering and research, specially in the areas of financial models or fluid simulations by solving partial differential equations. We notice that these computations are directly done in matrices and the computation time increases polynomially according to the size of the matrix. Moreover, it is significant in machine learning as the time required to find a least squares-fit decreases dramatically.

**Problem:**

To solve the system of linear equations.

**Quantum Solution:**

An efficient quantum algorithm was developed by Aram Harrow, Avination Hassidim and Seth Lloyd (HHL algorithm) which can approximate the solution vector with running time complexity of $O(\log N s^2 \kappa^2/\epsilon)$ while a classical computer requires $O(N s \kappa \log 1/\epsilon)$ running time where $N$ is the

size of the matrix, $\kappa$ is the condition number, $s$ is the non-zero entries per row or column and $\epsilon$ denotes the accuracy.

- Load the data $|b\rangle \in C^N$, i.e. perform the transformation

$$|0\rangle_{n_b} \longmapsto |b\rangle_{n_b}$$

- Apply Quantum Phase Estimation with

$$U = e^{iAt} := \sum_{j=0}^{N-1} e^{i\lambda_j t} |u_j\rangle\langle u_j|$$

  which makes the quantum state in eigenbasis of A as:

$$\sum_{j=0}^{N-1} b_j |\lambda_j\rangle_{n_l} |u_j\rangle_{n_b}$$

  where $|\lambda_j\rangle_{n_l}$ is the $n_l$- bit binary representation of $\lambda_j$.

- Add an auxialliary qubit and apply a rotation conditioned on $|\lambda_j\rangle$,

$$\sum_{j=0}^{N-1} b_j |\lambda_j\rangle_{n_l} |u_j\rangle_{n_b} (\sqrt{1 - \frac{C^2}{\lambda_j^2}} |0\rangle + \frac{C}{\lambda_j} |1\rangle)$$

  where C is the normalisation constant and $|C| < \lambda_{min}$

- Apply $QPE^\dagger$. Ignoring possible errors from QPE, this results in

$$\sum_{j=0}^{N-1} b_j |0\rangle_{n_l} |u_j\rangle_{n_b} (\sqrt{1 - \frac{C^2}{\lambda_j^2}} |0\rangle + \frac{C}{\lambda_j} |1\rangle)$$

- Now, measure the auxiliary qubit in the computational basis. If the outcome is 1, the register is in the post-measurement state

$$(\sqrt{\frac{1}{\sum_{j=0}^{N-1} |b_j|^2/|\lambda_j|^2}}) \sum_{j=0}^{N-1} \frac{b_j}{\lambda_j} |0\rangle_{n_l} |u_j\rangle_{n_b}$$

  which corresponds to the solution up to a normalisation factor.

- Apply an observable M to calculate

$$F(x) := \langle x| M |x\rangle$$

We also see that this HHL algorithm are highly useful for machine learning using a linear or non-linear binary clssifier or a support vector machine. Additionally, a quantum algorithm for Bayesian training of deep neural networks can give an exponential speedup using HHL.

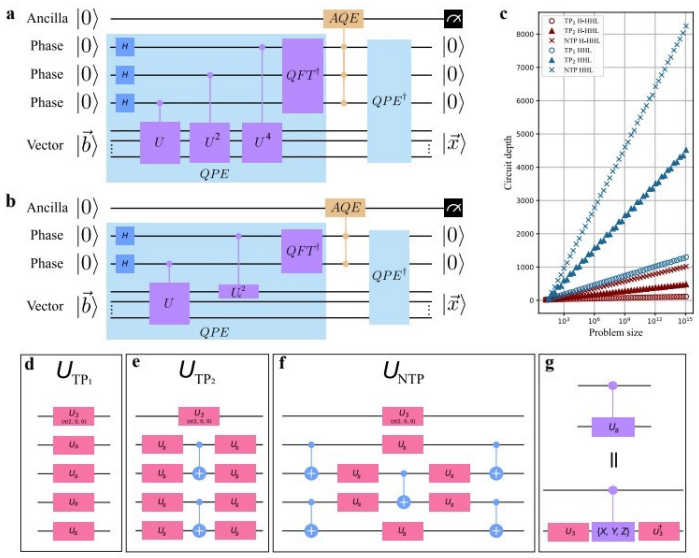



Figure 3.26: HHL Algorithm for solving linear equations

## 3.5 Hybrid quantum/classical algorithms

These are the algorithms that combine quantum state preparation and measurement with classical optimization to determine the ground state eigenvector and eigenvalue of a hermitian operator. This is basically implementing quantum algorithms with classical computations, where computations are based on measurements which give rise to accurate measurements. These algorithms give way to perform much complex problems by implemeting the previous algorithms and classical computation for manipulating the probability distribution in the most optimal way and finding the intial state easily.

### 3.5.1 Quantum Approximate Optimization Algorithm

[11]

**Value:**

These algorithms serve as a miniscule model of quantum annealing to solve problems in graph theory where we use classical optimization of quantum operations for an objective function. These algorithms have applications in all kinds of disciples including mechanics, economics and engineering. It also becomes quite intuitive as we implement the classical algorithms on the quantum computers giving a considerable speed-up. Moreover, they also serve as the building blocks of achieving adiabatic quantum computation.

**Problem:**

Some of the problems that come under this category are:

- find an optimal object out of a finite set of objects
- minimize the residual of a contraction (or projection) of the Schrodinger equation onto the space of two or more electrons to find the ground-or-excited-state energy and two-electron reduced density matrix of a molecule - based on classical methods for solving directly from the anti-hermitian contracted schrodinger equation.

- Max-Cut problem - partitioning nodes of a graph into two sets, such that the number of edges between the sets is maximum.
- Ising model

**Solution:**
We need to find the optimal parameters for of the least expectation value and we can obtain the value by measuring in the z-basis, so we operate the following procedure:

- Initialize $\beta$ and $\gamma$ to suitable real values.
- Repeat until some suitable convergence criteria is met:

  Prepare the state $|\psi(\beta,\gamma)|$ using QAOA circuit

  Measure the state in standard basis

  Compute $\langle\psi(\beta,\gamma)| H_P |\beta,\gamma\rangle$

  Find new set of parameters $(\beta_{new},\gamma_{new})$ using a classical optimization algorithm

  Set current parameters $(\beta,\gamma)$ equal to the new parameters $(\beta_{new},\gamma_{new})$

Thus, we develop a basic algorithm for preparing a general backbone of implementation in complex problems:

- Start with an initial state that is an equal superposition over all bitstrings (spins):

$$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{b\in\{0,1\}^n} |b\rangle$$

- Evolve with the cost Hamiltonian by implementing $U(H_C,\gamma)$ for an angle $\gamma$.
- Evolve with the mixer Hamiltonian by implementing $U(H_B,\beta)$ for an angle $\beta$.
- Repeat steps w and 3 p times with different parameters $\gamma_i,\beta_i$ at each step $i = 1,\cdots,p$ to form the state

$$|\gamma,\beta\rangle := \prod_{i=1}^{p} U(H_B,\beta_i)U(H_C,\gamma_i)\,|s\rangle$$

- Measure in the computational basis to compute the expectation of $H_C$ in this state:

$$F_p(\gamma,\beta) := \langle\gamma,\beta| H_C |\gamma,\beta\rangle$$

- Use a classical optimization algorithm to approximately compute the maximum or minimum value of $F_p(\gamma,\beta)$. Alternatively, if you have other methods to determine the optimal angles, you may use these.
- Samples from the output distribution of the circuit to get a set of bitstrings b. The most probable bitstrings encode the approximate optima for the cost function.

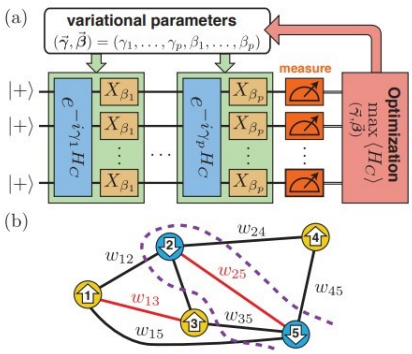



Figure 3.27: Schematic of a p-level Quantum Approximation Optimization Algorithm

### 3.5.2 Variational quantum eigensolver

[32]

**Value:**

With applications in mechanical engineering and finite element problems, we need approximations for a solution for boundary value problems, and thus, we develop an algorithm's goal is to prepare the ground state as a solution.

While using near-term quantum computers, we can define the solution as the ground state and we apply classical optimization to minimize the energy expectation of an ansatz state to find the ground state energy of a molecule (can be extended to find excited energies of molecules)

**Problem:**

To find the minimum eigenvalue of a matrix. (can be found by quantum phase estimation algorithm)

**Solution:**

We can perform the same results using Quantum Phase Estimation which gives an exact solution but it has two problems:

i it needs accurate approximate wavefunction as an input

ii it needs a large number of gates to represent the unitary propagator which makes the sequence of these gates too long

Both issues addressed by a direct minimization of the energy and s variational eigenvalue solver can be used on a photonic quantum processor. It sets up the qubits and measures the hamiltonian expectation value and then takes the value of hamiltonian expectation value to give a new angle for Quantum Circuit for optimum results.

Bounding the ground state:

We describe the Hamiltonian of the system by the Hermitian matrix and define the ground state of the system,$E_g s$ as the smallest eigenvalue associated with H. Our process includes approximating $|\psi_{min}\rangle$ by initial guessing and calculating its expectation value and therby updating the wave function as we tighten the bounds on the ground state energy of the Hamiltonian.

Here, we can represent this computation by a Hermitian matrix H with unknown minimum eigenvalue $\lambda_{min}$ associated with eigenstate $|\psi_{min}\rangle$, and we provide an estimate of $\lambda_\theta$ for bounding $\lambda_{min}$ such that

$$\lambda_{min} \leq \lambda_\theta \equiv \langle\psi(\theta)| H |\psi(\theta)\rangle$$

with classical optimization of the parameter $\theta$ for minimizing about the expectation value.

Thus, in variational method, minimizing the expectation value can be described as

$$\lambda_{min} \leq < H >_{\psi} = \langle\psi| H |\psi\rangle = \sum_{i=1}^{N} \lambda_i |\langle\psi_i|\psi\rangle|^2$$

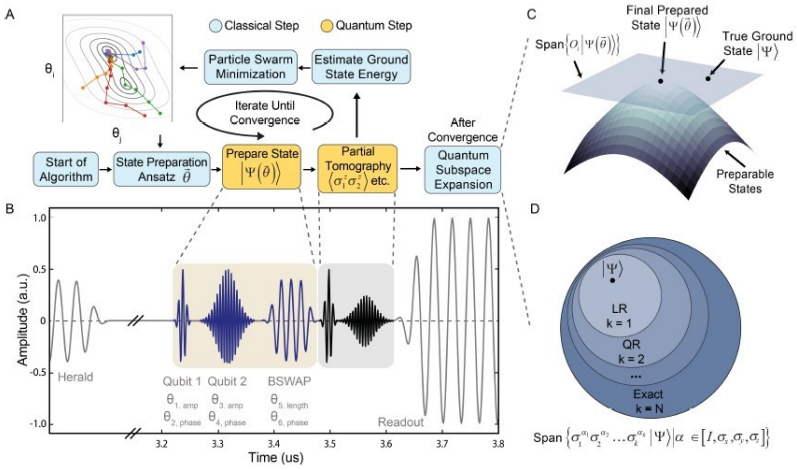



Figure 3.28: Representation of Variational quantum eigensolver with the associated quantum subspace expansion

There are three main challenges with this algorithm as well:

i unitary transformation is not so easy to find

ii the entire Hamiltonian measurement cannot be done

iii the Hamiltonian space is equivalent to the entire fock space.

This algorithm can further be improved to find the excited energies of molecules as well.

### 3.5.3 Contracted quantum eigensolver

[31]

**Value:**

Since Quantum phase estimation requires deep circuits with substantial error correction and adiabatic state preparation utilizes a slow and long time evolution with computational costs, so while VQE is super good, it suffers from high-dimensional classical optimization over a non-ideal surface, typically relying on derivative-free optimization, thus we move towards a different method of using contracted quantum eigensolver algorithm.

Contracted eigenvalue equations are a quantum analogue of classical methods for energies and reduced density matrices of ground and excited states. These are used for computation of ground and excited states of many-fermion quantum systems demonstrated on a quantum simulator and two IBM quantum processing units. This algorithm works on the principle of minimizing the residual of a projection of the Schrödinger equation onto the space of two(or more) electorns. Here, we find the solutions directly from the anti-Hermitian contracted Schrödinger equation.

**Problem:**

Solving the 2-RDM directly without storage of many-electron wave functions through ACSE

**Solution:**

Here, basically we use a contracted version by looking at the projection of the quantum eigensolver and use the algorithm for Quantum 2-particle anti-Hermitian contracted Schrödinger equation 2-particle reduced density matrix optimization

Given n=0 and $0 < \delta \leq 1$

Choose initial wave function $|\psi_0\rangle$

Repeat until $||^2\Lambda_n||$ is small.

- Prepare the auxialiary state $|\Lambda_n\rangle$ from $|\Lambda_n\rangle = e^{i\delta}$
- Measure ${}^2A_n$ from ${}^2A_N^{ij;kl} = Im \langle\Lambda_n| \hat{a_i^\dagger} \hat{a_j^\dagger} \hat{a_l} \hat{a_k} |\Lambda_n\rangle$
- Prepare $|\psi_{n+1}\rangle$ from $|\psi_n\rangle = e^{\epsilon \hat{A}} |\psi_n\rangle$
- Measure ${}^2D_{n+1}$ from ${}^2D_{n+1}^{pq;st} = \langle\psi_{n+1}| \hat{a_p^\dagger} \hat{a_q^\dagger} \hat{a_t} \hat{a_s} |\psi_{n+1}\rangle$
- Iterate Steps 3 and 4 to minimize the energy with respect to $\epsilon$
- Set n = n+1.

## 3.6 Quantum machine learning

[28]

We understand that machine learning is one of the most promising fields right now where a machine creates a model to interpret results of new inputs based on the previous given data and thereby researchers have developed a few methods in quantum computing for effective computations. Although there are unlimited applications but some immediate applications can be found in spam mail filters, iris recognition for security systems, financial risks, consumer behaviours, etc.

When we describe quantum machine learning, it can be interpreted into 3 broad aspects:

- Machine learning on quantum computers
- Machine learning on classical algorithms inspired by quantum mechanics
- Classical machine learning on quantum data

While the most intuitive way to move forward in quantum machine learning is by developing quantum versions of known classical machine learning algorithms since we already have the framework for computations in classical algorithms, quantum computers can be efficiently used for solving tasks like:

- linear algebra simulation with quantum amplitudes
- machine learning algorithms based on grover search
- quantum-enhanced reinforcement learning
- quantum annealing
- quantum sampling techniques

- quantum neural networks
- hidden quantum markov models
- fully quantum machine learning

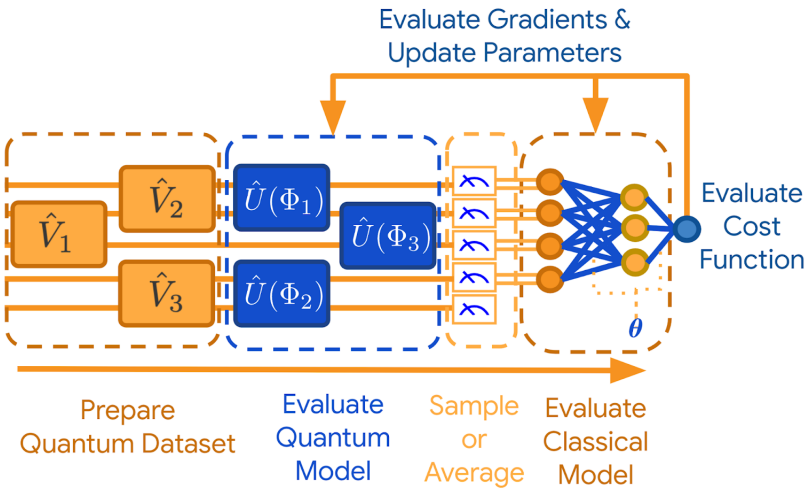



Figure 3.29: Quantum machine learning generalization

We can comprehend quantum computers like neural networks - using and training models like neural networks; in the field of differentiable programming which is the basis of deep learning - a programming paradigm where the algorithms are not hand-coded, but learned; and also with applications in quantum chemistry or quantum optimization with development of software libraries like tensorflow, pytorch, etc.

With principles in supervised or unsupervised machine learning, we can see their immediate prospective utilizations of quantum computing as:

- Quantum algorithms eg pattern recognition
- Preparing data in such a way that classical algorithm can solve it easier - eg k-nearest neighbour, support vector machines
- Quantum learning where quantum technology process input, output, data proposal of quantum neural networks as

    hopfield networks - derived from neuroscience rather than machine learning

    modified convectional neural networks

    quantum fuzzy feed forward networks

    pattern recognition by adiabatic computing

Practically speaking, quantum computers as AI accelerators have been constructed and we perform machine learning on near-term quantum devices like special purpose hardware like Application-Specific Integrated Circuits(ASICs) and Field-Programmable Gate Arrays(FPGAs). Google AI is the market leader in R&D right now.

# Chapter 4

# Physical realizations of a quantum computer

With great news bubbling up in the field of quantum computing, we need to actually realize these models and algorithms to perform actual computations and need to understand the creating of a qubit, i.e. the superposition of two quantum states, manipulation of the qubit and measurement to get a classical result. While we realize quantum computation physically, we need to create a balance between cohesion of different qubits to perform a computation and decohesion of these qubits when we don't want them to interfere.

Seeing this great potential of quantum computing, many countries and companies around the world are investing loads of time and money into building a practical quantum computer. With this, we note some important recent events by different countries -

- **Israel** announced the investment of 400 million dollars for a 5 year national quantum initiative in 2019 and is currently working on it's first quantum computer consisting of 30-40 qubits with the funding of 60 million dollars.
- **USA** has introduced a National Quantum Initiative Act with a funding of 1.2 billion dollars, inclusive of 625 million dollars for the Department of Energy to build 5 quantum computing centers across the US. Moreover, the companies IBM, Microsoft, Intel, Applied Materials and Lockheed Martin have invested 340 million dollars for the purpose of quantum computing.
- **UK** have also been at the forefront of quantum computing and the first quantum computer is built which is commercially available located in Abingdon in Oxfordshire with a funding of 10 million pounds (experts from Oxford, London, Bristol and Edinburgh) and companies like Rigetti Computing alongside Oxford Instruments, Standard Chartered, Phasecraft have been working for the same with the University of Edinburgh. The UK government has also announced 38 new projects benefiting from over 70 million pounds.
- Other countries like **China, Germany, Canada, India, Japan, etc** have invested heavily for the development of quantum computing. While Germany have invested 2.4 billion dollars for ten corporations that are co-founding the quantum technology and application consortium to develop fundamentals of quantum computing into use cases, China invested 10 billion dollars for this development, and Canada and Japan invested 2.2. billion dollars and 14 million dollars respectively. India is also developing quantum computing in association with Finland with leading cooperation between IISER and Aalto University.

With the understanding of the basic setup of the quantum computer, we need to approach to building a practical quantum computer and first need to construct a basic layout of creating a quantum state, i.e. a state where the qubit used is in a superposition of two states. Also, we need to physically realize our qubits and quantum algorithms into a complete quantum computer.

## 4.1 Set of rules

With the varied approaches to quantum computation, we need to establish a set of rules according to which we can define the criterion in a successful quantum computation. We define the rules according to Divincenzo's criteria:

For quantum computation:

- a scalable physical system with well characterized and scalable qubits
- the ability to initialize the state of the qubits to a simple fiducial state
- long relevant decoherence times
- a universal set of quantum gates
- a qubit-specific measurement capability

For quantum communication:

- the ability to interconvert stationary and flying qubits
- the ability to faithfully transmit flying qubits between specified locations

## 4.2 Scale of Comparison and Measurement

Now, we need a scale for comparison of these quantum computations. According to our knowledge, there are some basis for comparison, e.g. number of qubits used, error rate of qubits, cross talk between qubits, connectivity, systematic errors and efficiency of compiler.

At present, the comparison of different architectures is done by a benchmarking scheme proposed by IBM called "Quantum Volume". It is the measure used to test the efficacy of a quantum computer and is defined by the largest square circuit a quantum computer can solve.

Recent high scores:

| **Time of announcement** | **Company** | **Quantum Volume Score (Square Circuit)** |
|---|---|---|
| January 2020 | IBM | 32(5x5) |
| June 2020 | Honeywell | 64(6x6) |
| August 2020 | IBM | 64(6x6) |
| November2020 | Honeywell | 128 (7x7) |
| December 2020 | IBM | 128 (7x7) - 127 qubits |
| March 2021 | Honeywell | 512 (9x9) |
| July 2021 | Honeywell | 1024 (10x10) |
| December 2021 | Quantinuum (Honeywell + Cambridge Quantum) | 2048 (11x11) - 12 qubits SYSTEM MODEL H1-2 right now |

However, quantum volume does not take the computation time into consideration and thus, there is a need for other metrics for comparison between quantum computers, for which IBM has

proposed another metric called CLOPS(Circuit Layer Operations Per Second) which is the quantum version of classical FLOPS.

**Note:** The metrics we produce for comparison of quantum computations is checked for accuracy with classical simulations, but this becomes reduntant as quantum computers get advanced.

With the understanding of the metric for measuring quantum computation, we can understand the demonstration of quantum supremacy declared by Google in 2019.

> "Since the fundamental rules of computing have changed, the demonstration took place in 3 steps: (i) pick a circuit, (ii) run it on the quantum computer and (iii) simulation the quantum operation on a classical computer. As the complexity increases, the classical computer breaks down and could not simulate the computations, and that point was termed as quantum supremacy. Google developed a complicated machine which consists of the quantum chips, cryostats needed for these chips, control electronics and software, built in Santa Barbara, California. Sycamore is the quantum processor composed of 54 qubits (usable 53 qubits) made of superconducting loops was used to declare quantum supremacy by Google through their paper published in Nature on $23^{rd}$**October**2019. The team led by Dr. John Martinis checked the outputs from a quantum random-number generator (random operations on the 53 qubits giving $2^{53}$ possible computations where the process is so complex that it is impossible to calculate the result from first principles, though owing to the interference between the qubits result in some results being more likely) and declared that the computation that the quantum computer did in 3 mins 20 seconds, would take thousand years for a supercomputer (although IBM claimed that a supercomputer can perform the same in 1.5 days).

They also said that

> "mankind is pretty good at using advanced tools for finding practical applications like the space race started with a satellite orbiting the Earth was pretty much doing nothing but now it led to exceptional applications like a communication network, GPRS, etc."

and thus developments in quantum computing might be considered as the **"quantum race"**, the race for this decade.

## 4.3 Obstacles

Its really important to understand the obstacles in achieving successful computations in a quantum computater:
Coherence & Decoherence - we want the qubits to perfectly entangle with each other but not with the environment;
Minimize noise - we want to minize the noise in the quantum circuit which creeps in the form of cosmic rays, radiation, heat and rogue particles;
Scalability - we need to manipute and measure the qubits in a perfect manner.
One current solution proposed to overcome the obstacles is to use quantum error correction on fault tolerant quantum computers to collectively create a perfect logical qubit(about 100 to 1000 error quantified qubits combined).

According to the Google Technology blog, there can be roadmap about quantum computing:

- Implement error correction - combining several qubits to create a error corrected qubit which is lower noise

- Show error correction gets better with more qubits
- Make 1 logical qubit with endless coherency
- Make 2 logical qubits with 2 qubit operations - quantum transistor
- Tile thousands of logical qubits

Each of these tasks is a huge engineering challenge and right now, we are currently working with the first 2 steps. We relate to these assertions that creating high quality qubits with less noise is very important which is done by a few companies - IBM, Google and Quantinuum at the forefront.

## 4.4 Real-life quantum computers

Here, we describe the different approaches to create a superposition of quantum states and their manipulation and measurement to make computations possible. We also understand about the type of computation for which a particular setup is used. We elaborate on the work of the companies working on those type of quantum computers. Each type of quantum computer have their own advantages and disadvantages and thus relay their best use for solving different kinds of problems.

### 4.4.1 Superconducting Quantum Computers

**Introduction:**

With the most technological advancements in this type of quantum computing, it is apparent that superconducting QCs are at the forefront in terms of scalability and the current developments. These are the types of solid state electrical circuits where a Josephson junction acts as a passive circuit element and is implemented in an electronic circuit directly to form a qubit. Furthermore, according to the feature of the qubit used, the type of superconducting qubit is divided into 3 categories [17]:

i Charge qubits

ii Flux qubits

iii Phase qubits

Based on these qubit archetypes, new structures have been built as superconducting qubits such as Transmon-type qubit, 3-JJ flux qubit, C-shunt flux qubit, Fluxonium, $0 - \pi$ qubit, and hybrid qubit.

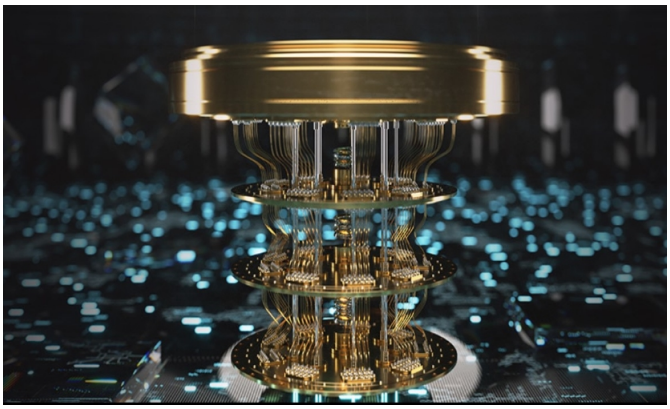


Figure 4.1: Superconducting quantum computing

**Advantages:**

- High designability - electric circuit is easily designable and adjustable using capacitors, inductors and Josephson junctions.
- Scalability - preparation is based on the exisiting semiconductor microfabrication process. advanced chip-making technologies used for high quality devices
- Easy to couple - circuit nature allows easy coupling with other qubits, capacitors and inductors
- Easy to control - operation and measurement compatible with microwave control

**Disadvantages:**

- short cohence times due to tunability and large size of superconducting qubits
- these qubits are not true 2-level systems, thus error due to unwanted $|1\rangle$ to $|2\rangle$ transition.
- Need dilution refrigerators to maintain low temperatures.

**Quantum Memory:**

We understand that the josephson effect is observed as a macroscopic quantum phenomenon between two superconductors placed in proximity with a barrier between them, and when supercurrent flows through this barrier continuously without any voltage applied, the device is known as a Josephson junction. The barrier can be an insulator, a non-superconducting metal or a physical constriction that weakens superconductivity at the contact point.

The wave functions of Cooper pairs in the superconductors can be implemented as

$$\psi_A = \sqrt{n_A}e^{i\phi_A} \text{ and } \psi_B = \sqrt{n_B}e^{i\phi_B}$$

and the two-state quantum system is represented through the Schödinger equation:

$$i\hbar\frac{\partial}{\partial t}\begin{pmatrix}\sqrt{n_A}e^{i\phi_A}\\ \sqrt{n_A}e^{i\phi_A}\end{pmatrix} = \begin{pmatrix}eV & K\\ K & -eV\end{pmatrix}\begin{pmatrix}\sqrt{n_A}e^{i\phi_A}\\ \sqrt{n_A}e^{i\phi_A}\end{pmatrix}$$

Physical apparatus example: A thin layer of aluminium oxide (an insulator) between two superconducting layers and becomes a superconductor when cooled below 1.2 K. The insulator layer is so thin (a few nm) that Cooper pairs can tunnel through it and couple the superconducting wavefunctions on either side of the barrier. Most of the circuits for superconducting qubits built so far consist of Josephson junctions and other components like capacitors connected by superconducting leads made of aluminium.

Considering Electrostatic energy of the cooper-pair as $E_J$ and Josephson coupling energy as $E_C$.

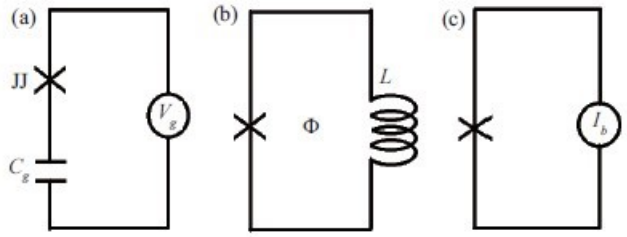



Figure 4.2: Superconducting qubit circuits (a) Charge qubit (b) Flux qubit (c) Phase qubit

| **Charge Qubit** | **Flux Qubit** | **Phase Qubit** |
|---|---|---|
| $E_J \ll E_C$ | $1 \ll \frac{E_J}{E_C} < 100$ | $E_J \gg E_C$ |
| Quantum Variable: | Quantum Variable: | Quantum Variable: |
| No. of cooper pairs crossing the josephson junction | Direction of current state in the superconducting loop | Phase difference between the electrodes of the junction |

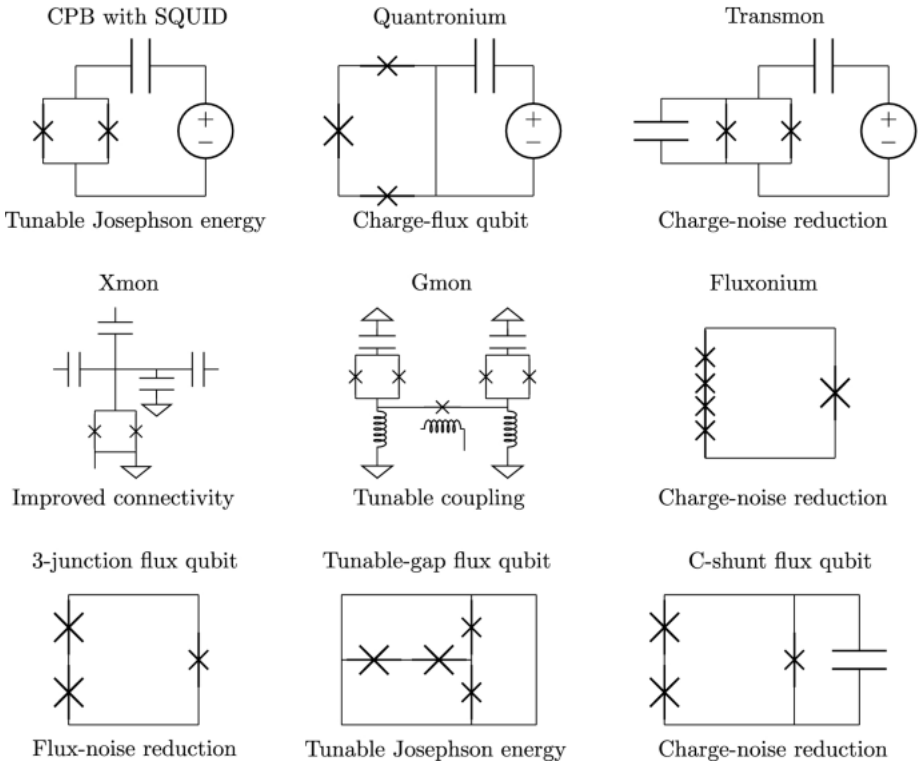



Figure 4.3: Different superconducting circuits generally used

**Transmon qubit:**

- most commonly used design
- a large capacitor in parallel with the superconducting quantum interference device(SQUID), along with a parallel resonator circuit and a secondary coil as the flux bias of SQUID.
- first built in 2007

developments on this type give rise to Xmon, Gmon, 3D transmon for long coherence times, fast control and better connectivity

**3-JJ flux qubit:**

- micrometer-sized loop with three or four Josephson junctions and superposition controlled by pulsed microwave modulation of the enclosed magnetic flux by current in control lines.
- reduced sensitivity to magnetic flux noise
- first built in 1999

**C-shunt flux qubit:**

- capactively shunted flux qubit (in 3jj flux charge noise is the main source of decoherence) - an additional capacitor shunted in parallel to the smaller josephson junction in the loop
- charge noise suppressed due to reduced charging energy

- first built in 2007

**Fluxonium:**

- a series array of large capacitance tunnel junctions are connected in parallel with a small junction.
- resolved inductance and offset charge noise problems because when the system oscillation frequency is below the plasma frequency, the series array of large junctions effectively behaves as an inductive wirecreating a low-pass filter
- first built in 2009

**$0-\pi$ qubit:**

- symmetrical circuit to obtain an interleaved double potential well and thus, the two ground state wave functions of a qubit are highly localized in their respective potential wells and do not disjoint each other.
- not sensitive to charge and magnetic flux noise since transiiton matrix elements between the corresponding two ground state energy levels are very small.
- designed in 2019.

Moreover, **Hybrid qubit** combines advantages of different quantum systems like coupling Nitrogen-vacancy centers in diamond to superconducting flux qubits to create effective quantum circuits for implementing faster computations with least noise errors.

An example of a superconducting qubit can be displayed in aluminium where the energy gap corresponds to 90 GHz at 20 mK temperature. It is an order of magnitude greater than the typical energy difference between the two levels in a superconducting qubit, so that qubits are be driven without breaking the cooper pairs. The behaviour of the electron superfluid is completely determined by a single quantum wavefunction whose amplitude gives the number of cooper pairs and the phase relates to the supercurrent (and any magnetic field presapplying logic operations on these qubits and thus, we understand the implementation of quantum gates using these superconducting qubits and the progress of high-fidelity gates.

Single qubit operations:

As these operations are based on the rotation of the qubit in 3d space, we can divide them into XY operations and Z opeent).

**Quantum CPUs:**

Here, we discuss the methods for computations on superconducting qubits.

**Single qubit rotations:**

XY operating principle:

Taking an example of a single Xmon qubit, we can couple microsources to Xmon by capacitance and when the qubit resonates with the microwave, the angle of rotation can be determined by the phase of the microwave drive.

$$H = -\frac{\hbar}{2}\Delta\sigma_z + \frac{\hbar}{2}\Omega_x(\cos\phi\sigma_x + \sin\phi\sigma_y)$$

where $\Delta = \omega(qubit frequency) - \omega_d(microwave frequency)$

Z operation:

Here, the Z line is directly connecting with a SQUID loop generating extra flux $\phi_e$ , the frequency of the qubit becomes

$$\omega_q/2\pi = E_1 - E_0 = \sqrt{8E_cE_J\cos\left(\frac{\pi\phi_e}{\phi_0}\right)}$$

and the corresponding evolution operator is

$$U = e^{-\frac{i}{2}\int_0^{t_0} -\omega_q(t)\sigma_z dt} = R_z(\int_0^{t_0} -\omega_q(t)dt)$$

**Two-qubit gates:**

Here we have the coupling term for same frequency qubits:

$$H_{couple} = \hbar g(\sigma_1^+\sigma_2^- + \sigma_1^-\sigma_2^+)$$

and the evolution operator is defined as:

$$U = exp(-\frac{i}{\hbar}\int_0^{t_0} H_{couple}dt) = exp(-\frac{i}{\hbar}H_{couple}t)$$

Thus, we can understand that for $t = \pi/2g$, we get iSWAP gate and if we divide this time by half, we get $\sqrt{iSWAP}$ gate.

**Implementation of 2 qubits:**

- Frequency tuning gates

  Grover search and Deutsch- Josza algorithms were achieved using adiabatic controlled-phase gates with 80% fidelity in 2009 which were improved to 99.4% later with randomized benchmarking, optimized pulse amplitude and frequency, and minimized two-state leakage. Also, non-adiabatic CZ gate were achieved with fidelities reaching $F = 99.54 \pm 0.08\%$ with $40ns$ gate time, and diabatic tuning used for getting iSWAP and CPHASE gates with fidelities upto 0.9966 and $18ns$ gate time.

- Cross resonance gates

  Here, an entangling state for fixed frequency superconducting qubits was achieved and implemented by applying a microwave drive to a system of two coupled qubits, giving rise 2 methods: (i) using quantum process tomography for 81% gate fidelity, and (ii) complete RB characterization of two-fixed frequency qubits for 93.47% fidelity.

- Parametric gates

  Here the two-bit gates are produced using parametric modulation and we can mix DC and AC drive to modulate the flux bias of the two-qubit system to drive the populations.

- Resonator-induced gates

  These provide us with an alternate method with producing an all microwave control process multiqubit gate. Here the qubits are statically coupled to the same driven bus resonator, which allows a high degree of flexibility in qubit frequencies and during operation, cavity state evolves from its initial state and finally returns to vacuum state.

Moreover, other multi-qubit gates can be implemented using the same principles to extrapolate for multiple qubits, eg using microwave resonator for toffoli gate with $68.5 \pm 0.5\%$ fidelity or by creating CCZ or CCCZ gate using QPT algorithms.

**Measurement:**

We can understand that we can use charge measurement, flux measurement and inductance measurement depending on the QED circuit architecture and thus can classify measurement methods according to the computation required

- Real-time quantum feedback: potential for quantum error correction and maintaining quantum coherence; readout operations, analysis of readout data, and generation of feedback operations must be completed before decoherence
- Dispersive readout: measure transmission coefficient of the readout resonator feasible way for quantum non-demolition readout of superconducting quantum computing
- High-fidelity single-shot readout: single output measurement with really high fidelity, 4 types - (i) purcell filters, (ii) josephson parametric amplifier, (iii) traveling wave parametric amplifier, (iv) impedance transform of parametric amplifier

Moreover, with quantum computers, there is a need for quantum error correction which is achieved through surface code (4 qubit parity measurements) and bosonic codes (infinite dimensionality of bosonic hilbert space), etc in superconducting quantum computers.

**Relevant Work and Developments:**

Here, we mention all the major companies working in these superconducting quantum computers along with their public announcement of the recent number of qubits that they have successfully achieved for computation(even though that no of qubits doesnt tell us about the error rate or quantum volume).

| | | | |
|---|---|---|---|
| **IBM-127** | **Google - 53** | **Intel Qutech - 49** | **UST of China - 66** |
| **Alibaba Quantum Laboratory - 11** | **Rigetti - 80** | **D-wave(Annealing) - 5760** | **Quantum Circuits** |
| **Bleximo** | **SEEQC** | **Alice & Bob** | **Origin Quantum** |
| **Oxford Quantum Circuits** | **Quantware** | **IQM Quantum Computers** | **Amazon** |
| **Raytheon BBN** | **Northrop Grumman** | | |

### 4.4.2 Quantum dot Quantum Computers(Also called Silicon Spin quantum computers):

[2]

**Introduction:**

As the theory of quantum computing links the elements of physics, mathematics and computer science, we delve into the possibility of using quantum dots for realization of qubits and quantum logic gates on two-electron spin states in coupled quantum dots. Here, the qubits are formed from

the quantum states of electrons or excitons(a bounded electron-hole system) where the higher and lower level correspond to ground state and excited states of the concerned qubit.

**Advantages:**

- Easy performance of read/write operations with visible light photons in emission/absorption processes
- The possibility of turning and controlling their electronic properties by changing the external electromagnetic fields.
- Fabrication is a natural extension of present semiconductor technologies
- Easily integratable with the existing hardware.

**Disadvantages:**

- Short decay time of the exciton
- Low transmittance may stay untectable or may demand high-sensitivity detection systems.

**Quantum Memory:**

Quantum dots are a semiconductor nanostructures ($< 1\mu m$, typically between 10 nm and 100 nm) which create a potential in all three space dimensions to confine charge carrier motion to a potential well of certain depth. These acts like a quantum harmonic oscillator and we get higher and lower energy levels which can then be used for quantum computations.

Now, while an electrostatic quantum dot can be of 2 types - pillar shaped quantum dots or capped quantum dots, the confinement potential V is parameterized as

$$V = -V_0 exp[-(r/P)^p - (|z|/Z)^p]$$

where $V_0 > 0$ is the potential well depth, $r = \sqrt{x^2 + y^2}$, $p > 1$, R and Z are the potential range limits in spatial coordinates. [$p = 2$ for Gaussian potential and rectangular for $p > 10$]

Now, electrons or excitons confined due to this potential serve n the quantum dot form and localized bound states define the discrete energy levels and the working quantum principle of these type of artificial atoms is quantum tunneling. Thus, a quantum dot is the basic memory unit in these realizations of a quantum computer.

We also understand that the quantum states can be represented though an empty conduction band, and a fully filled valence band where communication occurs through photons. The general chip materials used for creating a quantum dot are Silicon, Gallium Arsenide, Silicon Carbide and Diamond.

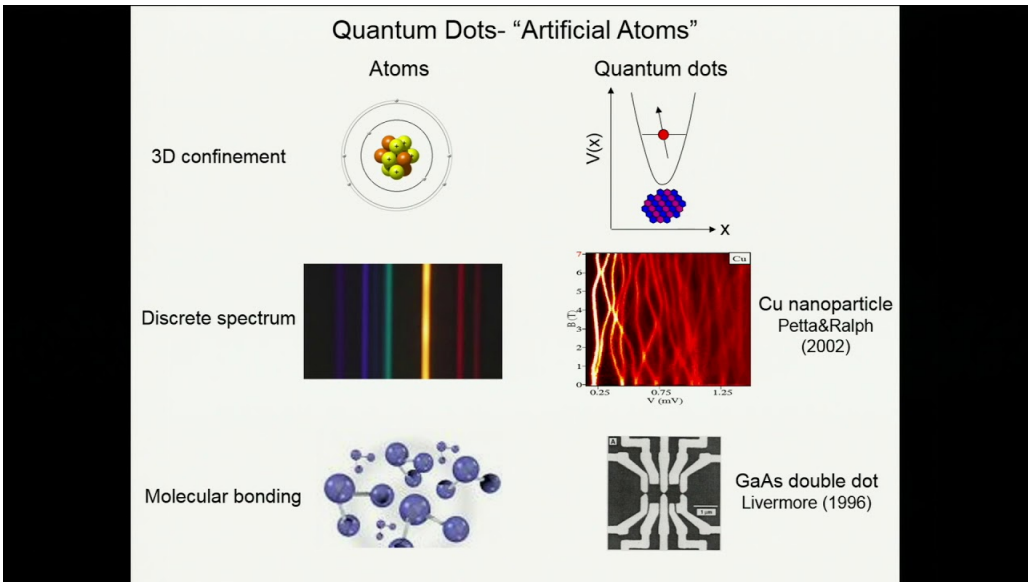



Figure 4.4: Representation of a quantum dot

**Quantum CPUs:**

Since quantum dots are tiny pieces of semiconductor crystal containing thousands of atoms, which behave like atoms having electron energy levels that can absorb and emit light at discrete wavelengths, thus when illuminated with ultraviolet light a quantum dot can be excited to a higher energy state and when it drops back down to its ground state, it can emit a visible photon allowing quantum dots to produce glow with vivid colours.

Also, when brought close to each other, they show complex quantum behaviour like interactions that stabilize excitons, which are quasiparticles (electron and a hole created by exciting an electron). Long-lasting excitons can have applications ranging from photocatalysis to quantum computing.

now, using the electron spin states to construct the qubits, logic operations can be operated in two ways -

- either directly with the application of the spin magnetic dipole coupling with the magnetic field, or
- indirectly with the application of symmetry properties of the many-electron wave function. (the indirect application of spin to represent the qubit is based on the change of the sign of the wave function during the exchange of the space-spin coordinates of two electrons)

So in the two-electron system, the spin singlet state (antisymmetric against the spin exchange) possesses a different (usually lower) energy than the spin triplet states (symmetric respect to the spin exchange) & logic operations done with the use of photon emission and absorption.

Giving rise to the field of spinotronics for implementation of biexcitons where spin transistors are designed for the application of spin states of quantum-dot confined electrons, very long relaxation time in the absence of external fields, and fairly long decoherence time ($t_{decoh} \simeq 1\mu s$) have been realized corresponding to easy manipulation of the spin by the external field.

For the implementation of the CNOT gate operation, the computational basis is formed from the eigenstates of the z component of the electron spin, and we manipulate the two-electron system

in the two coupled quantum dots. Here, hamiltonians are defined as:

$$H = H_1 + H_2 + H_{int}$$

where $H_j = \omega_j s_{z,j}$ ($\omega_j = g_j^* \mu_B B_j / \hbar$); $H_{int} = (4/\hbar)\Omega_{s_{z,1} S_{z,2}}$ defines the coupling.

The spin operators $s_{z,1}$ fulfill the eigenequations

$$s_{z,1} |0, l\rangle = +\frac{\hbar}{2} |0, l\rangle , s_{z,1} |1, l\rangle = -\frac{\hbar}{2} |1, l\rangle$$

where the spin-states $|k, l\rangle = |k\rangle \otimes |l\rangle$, and we have similar equations for $s_{z,2}$ provided $\omega_1 \neq \omega_2$

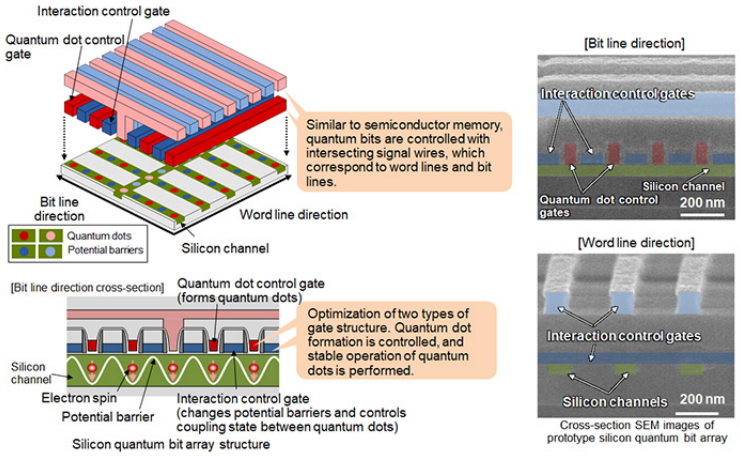



Figure 4.5: Computing through quantum dot principles

According to various experiments around the world, there are other methods for realization of spin qubits:

- measurement of spin via the measurement of charge
- measurement of a spontaneous magnetisation of the quantum dot
- electron spin resonance
- measurement of singlet triplet splitting with the help of a Faraday rotation

Since the practical processes involve thousands of atoms each hosting multiple electrons which prevents from capturing the characteristics of all exciton formation and recombination, thus Krause, Bande and Tremblay approximated the process though simulations which revealed how the quantum dot pairs absorb, exchange and store light energy. They also found how excitons can be stabilized by applying a sequence of ultraviolet and infrared pulses to quantum dots. While an initial ultraviolet pulse can generate an exciton in one quantum dot, a subsequent pulse can shift the exciton to a nearby quantum dot where the contained energy can be stored.

The team simulated interactions between three pairs of germanium/silicon quantum dots, which had different shapes and sizes. They now plan to create more realistic simulations that will allow them to model how environmental factors like temperature influence interactions. Through further improvements, we could like to see their application in qubits that can reliably store and read out quantum information and photocatalysts that absorb sunlight, facilitating reactions that produce hydrogen gas as a carbon-free fuel source.

**Relevant Work and Developments:**

Here, we mention all the major companies working in these superconducting quantum computers along with their public announcement of the recent number of qubits that they have successfully achieved for computation(even though that no of qubits doesnt tell us about the error rate or quantum volume).

| | | | |
|---|---|---|---|
| **Qutech** | **Intel** | **Cea-leti** | **Hrl laboratories** |
| **Photonic** | **Quantum Motion** | **Riken center for quantum computing** | |

### 4.4.3 Linear Optical Quantum Computers - photonic:

[19] [24]

**Introduction:**

With special applications in the areas of cryptography and secure communications, another approach in quantum computing processes information in the form of single photons as qubits. Since we already have a framework of optical fibres already, this kind of approach becomes apparent in terms of developments. They are based on linear optical elements on a quantum circuit and is referred to as "probabilistic devices" as they have a probability of failure and the results are adjusted accordingly.

This type of computation acts as an integration of quantum computation and quantum communication and the basic unit ranges from cat-state logic to encoding a qubit in a harmonic oscillator and optical continuous-variable quantum computing.

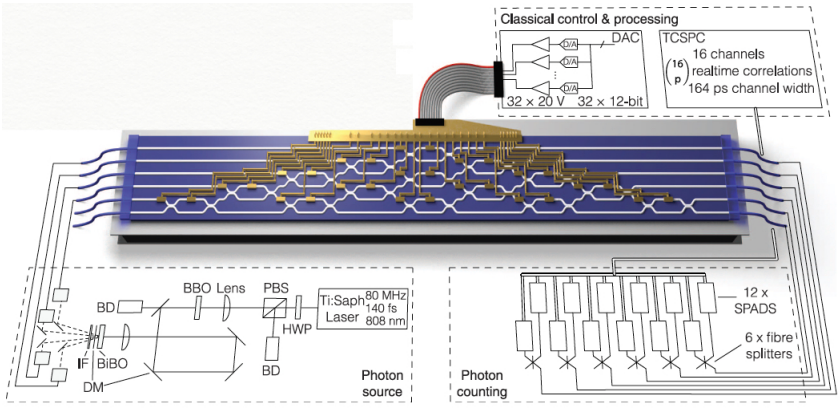



Figure 4.6: Representation of a linear optical circuit

**Advantages:**

- Ability to connect logic and memory devices using optical fibers in analogy with the use of wires in conventional electronic circuits.
- Smallest unit of quantum information i.e. the photon is potentially free from decoherence

- Level of error detection is accurate since we detect exactly number of photons.

**Disadvantages:**

- Difficult implementation of quantum logic logic gates needed to perform calculations.
- Photons do not naturally interact with each other therby limited success probabilities of quantum gates for these interactions.
- Need to know the minimum overhead in cluster state production.

**Quantum Memory:**

Single photon sources are the fundamental building blocks of these computations where they not only generate the control and target photons but also the ancilla photons. Thus, we need to build a quantum network of photonic elements for communication in this type of computation and the building blocks are beamsplitters, half and quanrter wave plates phase shifters, etc.

The quantum-mechanical plane-wave expansion of the electromagnetic vector potential is usually expressed in terms of the annihilation operators $\hat{a_j}(k)$ and their adjoints - creation operators:

$$A^{\mu}(x,t) = \int \frac{d^3k}{\sqrt{(2\pi)^3 2\omega_k}} \sum_{j=1,2} \epsilon_j^{\mu}(k)\hat{a_j}(k)e^{ikx-i\omega_{k^t}} + H.c.$$

A single-mode phase shifter changes the electromagnetic field in a given mode:

$$\hat{a_{out}}^{\dagger} = e^{i\phi\hat{a_{in}}^{\dagger}\hat{a_{in}}}\hat{a_{in}}^{\dagger}e^{-i\phi\hat{a_{in}}^{\dagger}\hat{a_{in}}} = e^{i\phi}\hat{a_{in}}^{\dagger}$$

with the interaction Hamiltonian $H_{\phi} = \phi\hat{a_{in}}^{\dagger}\hat{a_{in}}$

Also, we can describe the beam splitter as it parameterizes the probability amplitudes and yields an evolution as:

$$\hat{a_{out}}^{\dagger} = \cos\theta\hat{a_{in}}^{\dagger} + ie^{-i\phi}\sin\theta\hat{b_{in}}^{\dagger}$$
$$\hat{b_{out}}^{\dagger} = ie^{i\phi}\sin\theta\hat{a_{in}}^{\dagger} + \cos\theta\hat{b_{in}}^{\dagger}$$

corresponding to reflection and transmission with Hamiltonian of the beam-splitter evolution being:

$$H_{BS} = \theta e^{i\phi}\hat{a_{in}^{\dagger}}\hat{b_{in}} + \theta e^{-i\phi}\hat{a_{in}}\hat{b_{in}^{\dagger}}$$

Moreover, using quarter plates and polarizers, we can build polarized beam splitters for different polarization directions.

Using this knowledge, a single photon can be used as a qubit in two different modes and can be represented in two ways:

- In dual-rail logic, the states can be portrayed in accordance to the two spatial modes $|0\rangle_L = |1\rangle \otimes |0\rangle = |1,0\rangle$ and $|1\rangle_L = |0\rangle$
- Corresponding to internal polarization degree of freedom, the states can be portrayed as $|0\rangle_L = |H\rangle$ and $|1\rangle_L = |V\rangle$

In simple words, we build a storage ring (optical fiber in a loop) which is similar to a memory and the photon's direction around the ring can dictate the qubit value or like in quantum key distribution, we can use the polarization feature of the photons as a quantum bit which is relative to the plane of measurement.

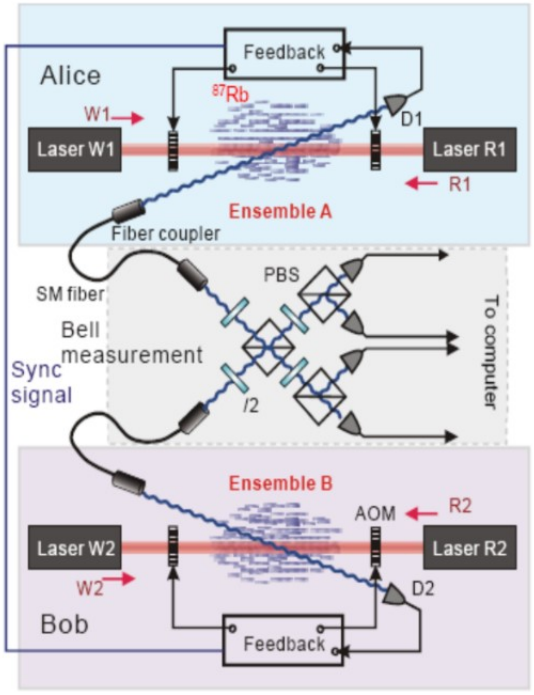



Figure 4.7: Circuit using linear optical elements

**Quantum CPUs:**

We understand that we need both single-qubit and two-qubit operations to buid a practical quantum computer.

**Single qubit gates:**

We can easily implement the Pauli operators or rather any operator $e^{i\theta\sigma_j}$ as a rotation in the Bloch sphere by using phase shifters, beam splitters and polarization rotations.

**Two qubit gates:**

We understand that implementing two-qubit gates in this type of computer is pretty problematic but can be fulfilled by using the creation and annihilation operators.

While there were many approaches to reach a solution, the most interesting one which could contain other approaches in its entirety and has potential to be built upon is the KLM protocol. The KLM protocol is a protocol in which probabilistic two-photon gates are teleported into a quantum circuit with high probability.

- Elementary gates

  Since the photons do not interact with each other, we cannot build deterministic two-qubit gates and thus the only way for influential behaviour is through the bosonic symmetry relation. According to the bosonic commutation relation with respect to a beamsplitter as:

$$|1,1\rangle_{in} \rightarrow_{trans} \cos^2\theta\,|1,1\rangle_{out}$$
$$|1,1\rangle_{in} \rightarrow_{refl} \sin^2\theta e^{i\phi}e^{-i\phi}\,|1,1\rangle_{out}$$

[for a 50:50 beamsplitter, we get exactly cancelled paths]

This is identical to

$$|q_1,q_2\rangle \rightarrow_{CZ} (-1)^{q_1 q_2}\,|q_1,q_2\rangle$$
$$|q_1,q_2\rangle \rightarrow_{CNOT} |q_1,q_2 \oplus q_1\rangle$$

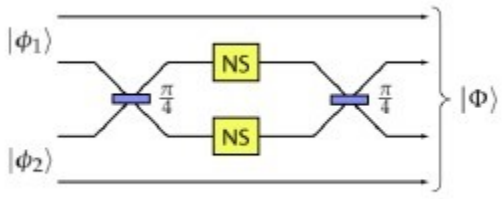



Figure 4.8: CZ gate from two NS gates and two beamsplitters

Similarly, we can form relations for other gates based on the commutator relation which can yield nonlinear sign(NS) gate, or Knill CZ gate, etc

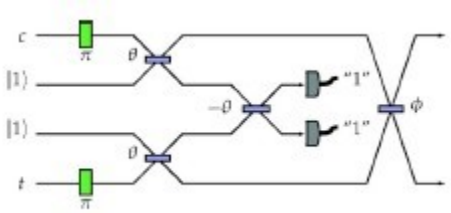



Figure 4.9: Knill CZ gate based on two ancillae photons and two detected photons

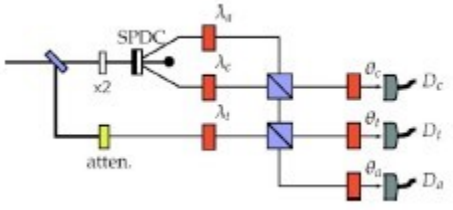



Figure 4.10: Schematic design of 3 photon CNOT gate

- Parity gates and entangled ancillae

Parity check gate is a special optical gate consisting of a single polarizing beam splitter followed by photon detection in the complementary basis of one output mode. Here, let a and b be the input modes, and c and d be the output modes, then this gate induces the transformation:

$$|H,H\rangle_{ab} \rightarrow |H,H\rangle_{cd}$$
$$|H,V\rangle_{ab} \rightarrow |HV,0\rangle_{cd}$$
$$|V,H\rangle_{ab} \rightarrow |0,HV\rangle_{cd}$$
$$|V,V\rangle_{ab} \rightarrow |V,V\rangle_{cd}$$

where $|HV,0\rangle_{cd}$ denotes a vertically and horizontally polarized photon that yield a parity check in the $(|H\rangle \pm |V\rangle)/\sqrt{2}$ complementary basis.

This gate enables to create Bell states and these probabilistic gates can increase their probability using feedforward protocols.

- We also understand that there are various other all-optical probabilistic quantum gates that have been realized like three-photon CNOT gate, destructive CNOT gate, parity check gate with two-photon conditional phase switch, etc

**Relevant Work and Developments:**

Here, we mention all the major companies working in these superconducting quantum computers along with their public announcement of the recent number of qubits that they have successfully achieved for computation(even though that no of qubits doesnt tell us about the error rate or quantum volume).

| | |
|---|---|
| **UST of china(no of photons in a boson sampler) - 113** | **Xanadu - 40** |
| **Psiquantum** | **Quix quantum** |
| **Orca computing** | **Quandela** |

### 4.4.4 Trapped ion Quantum Computers:

[6]

**Introduction:**

Ions traps have been prevalent since 1953 by trapping ions in a potential well using electromagnetic traps. For this, Wolfgang Paul and colleagues invented a Paul trap (won Nobel Prize Physics 1989) which is used to make highly precise atomic clocks where time dependent electric fields allow the potential walls to move.

As Shor proposed his algorithm for factoring very large numbers, implementation of this algorithm gave rise to quantum computation using individual atomic ions by Cirac and Zoller. Here, by confining the ions in a radiofrequency trap serve as quantum bits, we delve into a different kind of technology where quantum interations are observed macroscopically as we use the mechanics of ion trapping and the equations governing the interaction between electromagnetic control fields and ions.

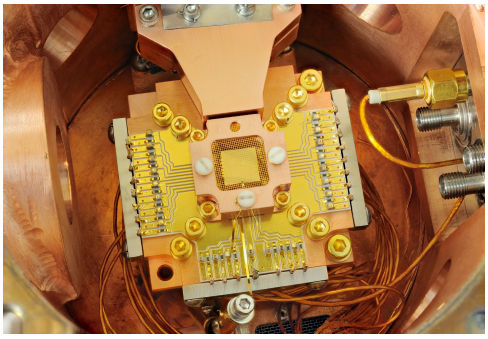


Figure 4.11: Picture of a trapped ion quantum circuit

**Advantages:**

- Long hyperfine qubit coherence times
- Very high fidelity for single and two-qubit gates achieved and thus good accuracy - very low error rates
- Manipulation and measurement is done directly and thus good connectivity - easy to entangle many qubits together
- High stability - even operate at room temperature

**Disadvantages:**

- Fairly slow - compared to other types of computation
- Difficult to scale as the complexity of many lasers, vacuums, and trapped ions rises with number of qubits

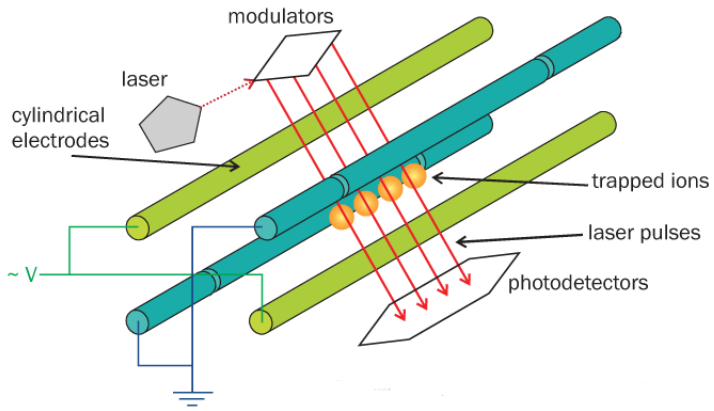



Figure 4.12: Basic representation of a trapped ion circuit

**Quantum Memory:**

This computation shows a lot of promise since it is a straightforward methodology for localizing atomic ions for long periods of time which can be used for observing quantum behaviour directly in our circuit. In this type of quantum computation, we have individual atoms trapped in ion traps which serve as a qubit. So firstly, we need to know the **ion traps** for particular qubits. So, ion traps can be of 2 major types

i Penning trap - a trap which provides confinement using static electric field in one axial direction and a parallel static magnetic field for the other two perpendicular, radial directions.

ii Paul trap - a trap which provides confinement with an oscillating electric field which sets up a ponderomotive confining pseudopotential in two or three dimensions. This can be achieved using 2 different layouts:

(a) point trap - using quadrupole electrode layouts that lead RF trapping in 3 dimensions giving one point as RF null.

(b) linear trap - using 2-dimensional RF trapping and 1-dimensional electric-field trapping giving zero RF field along a line.

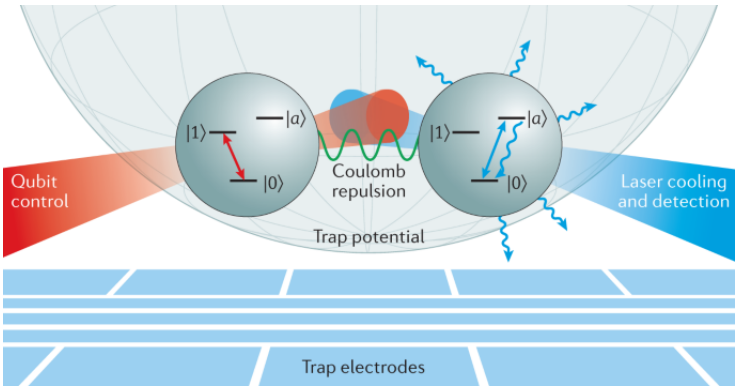



Figure 4.13: Representation of a trapped ion qubit

These traps first macroscopically designed was miniaturized using laser-etched insulating substrates, selectively coated with patterned metal electrodes to obtain smaller, more precisely defined structures, and multi-linear-segment array structures with hundreds of separate electrode segments, segmented circular rings, multi-site point trap arrays, and traps with electrodes with switchable or variable RF amplitudes or of varying geometry across a linear, segmented region for complex trap designs.

Now, the quantum states considered here are the **internal states** in mostly Group-II or Group-II-like atomic ions, i.e. the energy levels in the ion structure. Based on the interacting frequency, orbital energy levels and their lifetimes, we can create 4 major types of qubits:

**Zeeman Qubits**
(i) pair of states in the same electronic orbital and hyperfine level

**Hyperfine Qubits**
(i) pair of states in the ground state hyperfine manifold

(ii) energy levels separated by MHz frequencies

(iii) coherence times of 300 ms achieved

**Optical Qubits**

(i) one state in the ground state manifold and the other in a metastable D level

(ii) control wavelengths in the visible to near-IR-region

(iii) coherence times of 0.2 s achieved

(ii) energy difference in the range of microwave region

(iii) coherence times of 600 s achieved

**Fine-structure Qubits**

(i) pair of states in the D manifold

(ii) energy splittings in the THz range

(iii) coherence times of 1-100 ms achieved

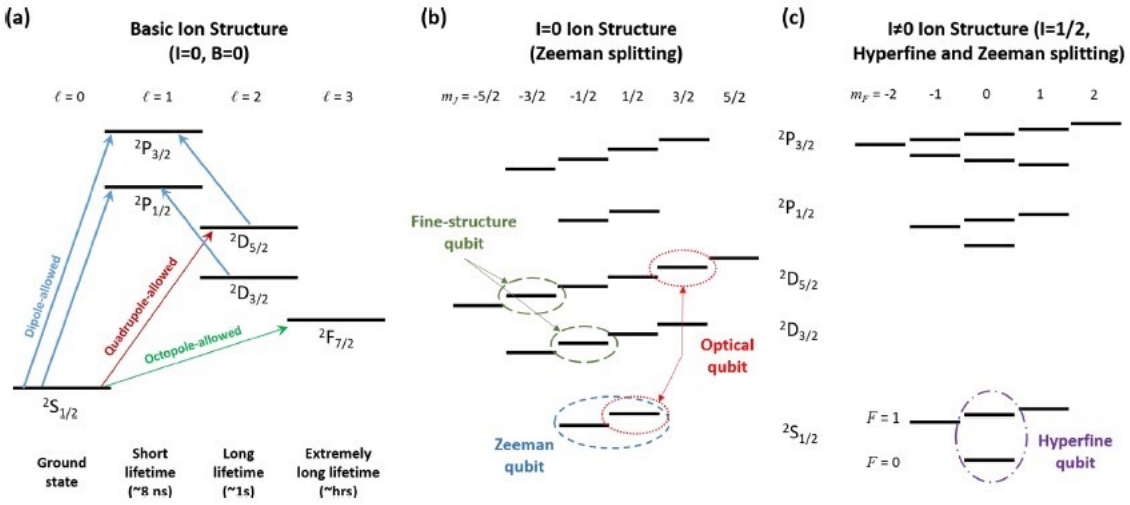



Figure 4.14: Representation of a the energy levels

Adding to this, many ions used simultaneously can form an ion chain where ions in a sufficiently spaced one-dimensional array and cooled to the point that motion is quantized. Through experiments, we find that best ions for our purposes are single-charged ions in group 2 - Calcium-40, Beryllium-9, Barium-138 used at university labs or [Ytterbium-171 used at Ionq & Honeywell] where the elements have 2 valence electrons, and their ionized version has one in the orbital and the valence electron is not so tightly bound to the atom, hence an optical qubit.

Moreover, trapped ions can take advantage of external, shared vibrational states in combination with the long-lived internal states where harmonic trapping potential of the vibrational states have MHz frequencies. With developments in Fock state interferometry to measure the typical fluctuations and drifts in trap frequencies, the fluctuations are found at $10^{-6}$ to $10^{-5}$ level in the tens to hundreds of seconds timescale giving increased stability to the qubits.

**Example:** Ca-40 ion pumped with 729 nm infrared laser with a half life of 1 second and our quantum operations take place in $\mu s$ to $ms$. The two quantum states are the stable ground state and the metastable excited state. The coherence times are longer for hyperfine qubits if Ca-43 hyperfine structure is used, but it will be complicated implementation and need more precision. The ions in a chain make multi-qubit state implementations and the entire ion chain behaves as a quantum harmonic oscillator.

**Quantum CPUs:**

Here, fine-tuned lasers can control the state of a single qubit and the trapped ions interact via vibrations felt by their changes and they can even become entangled.

**State preparation:**

First, we understand that an ion register has to be prepared in the desired initial state before applying the quantum operations, so ions are optically pumped to the desired initial state, taking advantage of photon absorption and emission selection rules.

**Single-qubit gates:**

Also, we understand that the interaction of the ions can be described by optical, raman, or microwave transitions refering to the type of computation and the recent sucesses with the respective method used is:

- Optical - a few $\mu s$ with fidelities upto 99.995%
- Microwave - $12\mu s$ with 99.9999% fidelity
- Zeeman single-qubit gates - RF drive with 99.9% fidelity in $8\mu s$

**Multi-qubit gates:**

Here, we need entanglement of internal and motional states of trapped ions which is achieved by coulomb interaction. Some of the prominent gates produced through trapped ions are:

- CZ gate(Cirac Zoller) - This is a controlled phase gate where the shared motional modes of ions are used as a bus to transfer quantum information. Here the ions required to be cooled to ground state of their collective motion, and individual addressing of each ion via multiple polarizations for the drive laser.
- Molmer-Sorensen gate(MS gate) - This gate generates a state-dependent force with bichromatic laser fields tuned near first-order sideband transitions, and their motional-state wavepacket executes a closed trajectory in phase space giving rise to a state-dependent geometric phase. Here, this gate can be used for ions that are not cooled to the motional ground state and entanglement among multiple ions can be generated using only global control lasers.
- Leibfried's geometric gate - This is a phase gate which uses a pair of detuned laser beams to generate a state-dependent force which traces a closed path in phase space. This too utilizes the shared motion of the ions to generate coupling between them and is insensitive to the initial ion motional state (but doesn't involve transition between $|1\rangle$ and $|0\rangle$ qubit states)

**State detection:**

Now, measurement can be done by shining a different laser at an ion well which causes any previous superposition to collapse and detection is made through this state-dependent fluorescence. The trapped ion is projected into either a so-called bright state that scatters many photons when illuminated with a detection laser or a so-called dark state that scatters very few photons and these scattered photons are collected by a high-NA lens for detection.

Example: : Light of 397 nm is provided and emitted when the state is in ground level and dark when in excited state where the states are in superposition according to Rabi oscillation and gates are applied through consecutive pulses with different times and phases.

**Relevant Work and Developments:**

Here, we mention all the major companies working in these superconducting quantum computers along with their public announcement of the recent number of qubits that they have successfully achieved for computation(even though that no of qubits doesnt tell us about the error rate or quantum volume).

| | | | |
|---|---|---|---|
| **Quantinuum - 12** | **IONQ - 32** | **Alpine Quantum Technologies - 24** | **Oxionics** |
| **Infineon** | **Universal Quantum** | **Oxford Ionics** | **Qscout** |

good with creating secluded environment, but have to be placed in spatial coordinates to control their position and the vacuum should be really good limiting scalability

### 4.4.5 Colour Centre Quantum Computers (Nitrogen valancy quantum computers):

[25]

**Introduction:**

This type of computation takes a slightly different approach by creating artificial atoms like nitrogen vacancy centers in a diamond, acting as a solid state qubit operating at room temperature for great strides in quantum computing and quantum sensing. They present a game-changing approach as they work on the same principle as trapped ion quantum computers with much more stabilized qubits and thus shows significant promise in the quantum race.

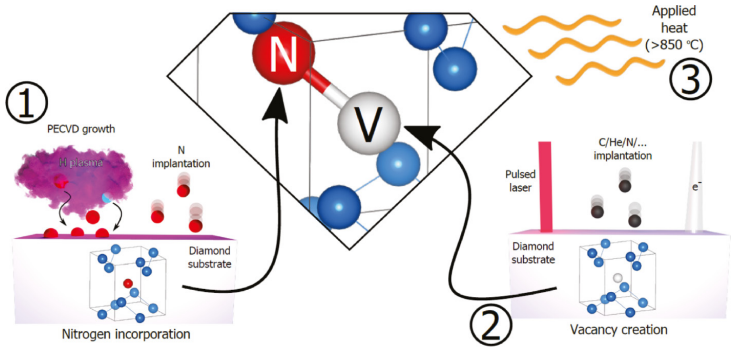



Figure 4.15: Basic representation of a colour center circuit

**Advantages:**

- Similar electronic structures, spectral lines, and spin properties because of well-defined properties of defects based on single atoms
- Larger availability of isolated vacancies enabled by Coulomb repulsion
- NV is coupled directly with photons and a real flying qubit can be produced
- Structures are very stable in time and do not change even during subsequent healing

- Operated at room temperature
- Qubits maintain their position even in technical failure
- Solid-state solution is desirable as connection eith current CMOS technology easy

**Disadvantages:**

- The coupling strength cannot be adjusted and is determined by the distance between the NVs
- Diamonds have limited scalability, electrical control, integration and fabrication

**Quantum Memory:**

**Environment:**

Since we realize that we need an isloated system to contain a qubit information to reduce error in quantum mechanical measurements, while ensuring the greatest possible control over it, we look towards a solid-state solution which can be easily connected with the current CMOS technology. Thus, defect-free isotopic $^{12}C$ diamond crystal(with bandgap of 5.4 eV) play as a host which provides vacuum-like conditions and a point defect center acts as an atom in a trap, suitable even at room temperatures.

Although imperfections in the crystal or impurity atons can cause quantum phase disturbance, we can still assert that all quantum devices have similar electronic structures, spectral lines and spin properties because of the well-defined properties of defects based on single atoms.

**Quantum state:**

Now, the defect centers in diamond exhibit quantum mechanical properites in terms of their spin states and it is found that there are 2 types of defect centers that can be controlled at room temperature (the spin state of SiV centers as well at low temperature but they have short coherence times):

- Nitrogen Vacancy centers (NV Centers)

  It comprises a nitrogen atom with a nuclear spin of 1 ($^{14}N$) or 1/2 spin ($^{15}N$) and a first neighbour carbon vacancy. Here, the electrons build a triplet state with a zero-field splitting of 2.87 GHz in the $NV^-$ state (advantage: $m = 0$ spin state exhibits different behaviour than $m = \pm 1$ spin state).

  The Hamiltonian of the NV center can be defined as:

$$H = DS_z + \gamma_S \vec{S}\vec{B} + \vec{S}\bar{\bar{A}}\vec{B} + \gamma_I \vec{I}\vec{B}$$

  Here, the ground state defines the triplet state and singlet state is reached via intersystem crossing from the excited state as spin polarizations takes place exactly via the singlet state(transition rates for $m = \pm 1$ are significantly stronger than for $m = 0$), thus after only a few excitation cycles, a spin polarization is achieved with 98% probability. As phonon interaction is suppressed, coherence times of several milliseconds are achievable in an isotopically pure diamond at room temperature.

- ST1 Centers

  [4]

These are the point defects in a diamond with bright fluorescence and a mechanism for optical spin initialization and readout, acting as a register of nuclear spins. Although the chemical structure is unknown, they have exceptionally high readout contrast. Here, charged color centers possess a singlet ground state and are transformed into a triplet state by excitation.

We observe that the triplets show a fine-structure at zero field in the optically detected magnetic resonance spectra and thus the spin-Hamiltonian of the triplet manifold is:

$$\hat{H} = D[S_z^2 - S(S+1)/3] + E(S_x^2 - S_y^2) + \gamma_e \vec{S} \cdot \vec{B}$$

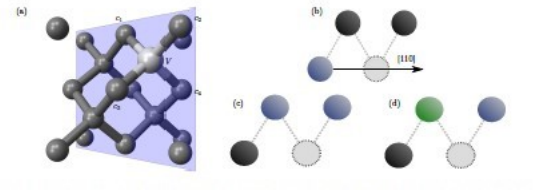


Figure 4.16: Cell of a diamond showing a vacancy

**Quantum CPUs:**

Since we understand NV centers in much detail, we would discuss the manipulation and measurement in reference to NV center quantum computing.

**Initialization:**

We understand that the diamond lattice prevents us from initializing the qubit states electronically and thus even though the initialization stage of these qubits is easy to fulfil, it is achieved only by means of a light pulse.

So, there is a 30% chance for $m = \pm 1$ state to undergo a non-radiative intersystem crossing to the singlet state and decay to m=0 state, and after 10 cycles, the NV center is polarized to 98% at room temperature. To achieve practical fidelity of 99.99%, we can change to low temperature or to a $^{13}C$ transferring spin state procedure.

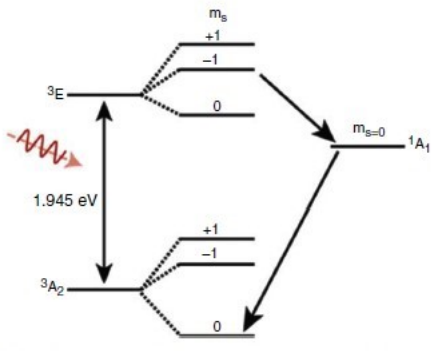



Figure 4.17: Representation of the energy levels of $NV^-$ center

**Single-qubit gate operations:**

We observe that the spin state of the NV qubit can be switched coherently by using a $\pi$- pulse, i.e. microwave pulse of a certain length and intensity, which represents a NOT gate.

**Multi-qubit gate operations:**

Since the resonant frequency is observed in reference to the spin state of nearby centers or nuclear spins, we can use a narrow-band microwave $\pi$-pulse to perform a controlled rotation(CROT) gate, or indeed with additional rotation to a CNOT gate. Here, the target qubit only flips when the target gate is resonant with the microwave field which happens only when the controlled qubit is the $|1\rangle$ state.

The best coherence times achieved using this method was using slightly n-type doped $^{13}C$ free diamonds to get $2ms$ at room temperature. Here, single-qubit gates achieved with 99.99% fidelity and double qubit gates with 99.2% fidelity in qubit systems in diamond or SiC crystals. With coherent control of up to 30 spins, entanglement and high quality quantum algorithms realized with 10 qubits.

Now, to establish realization of these gates, we need to establish the coupling for NV spin systems, and thus we see different approaches:

- magnetic dipole coupling of electronic NV-NV and nuclear NV-$^{13}C$ spins : the dipole-dipole interaction is given by:

$$H_{dip} = \frac{\mu_0 \gamma_e^2}{4\pi r_{AB}^3}[S_A S_B - 3(S_A + n_{AB})(n_{AB} S_B)]$$

  We see that NV-NV coupling occurs at 10 kHz for 30 nm separation, NV-$^{13}C$ at 12 MHz for the first shell of $^13C$, and NV-$^{14}N/^{15}N$ coupling at 2 and 5 Mhz in the ground state.

- direct NV-N-NV coupling : since electronic dark spins get included in the direct NV-NV coupling, we move towards NV-N-NV coupling or spin chain NV-N-NV-N...N-NV where overlap between NV center and the P1 center allows possible energy transitions resulting in resonant coupling for targeted spin exchange.

- NV-photon-NV coupling : photons directly coupled with NV can used at very low temperatures which makes the construction of a quantum network easy.

- Also, we can use charge state control of NV-$^{15}N$-NV-$^{15}N$ coupling according to their charged state nature. NV-$^{13}C$ multicoupling achieved at low temperatures using the resonant RF frequency between hyperfine interaction and the spin of $^{13}C$.

- Moreover, AFM tips mechanical control and electron bus system are two other methods for NV-x-NV coupling. Adding to this NV centers can be emplyed as storage elements for superconducting qubits which shows a lot of promise towards practical quantum computing.

**Measurement:**

We observe that measurement of the state here can be done by either an optical spin readout (generally a resolution of 250-400 nm $\sim \lambda/2NA$ is used) where single-shot readout can be obtained by excitation at a certain frequency, or an electron spin readout where the photocurrent of magnetic resonance is detected (only NVs with high suction coltages read out this way).

**Relevant Work and Developments:**

Here, we mention all the major companies working in these superconducting quantum computers along with their public announcement of the recent number of qubits that they have successfully achieved for computation(even though that no of qubits doesnt tell us about the error rate or quantum volume).

| | |
|---|---|
| **Qutech** | **SQC** |
| **Quantum Brilliance - 2** | **International Iberian Nanotech Lab** |

### 4.4.6 Neutral Atoms in Optical Lattices:

[10] [16]

**Introduction:**

This approach looks into computational with a qubit built from neutral atoms trapped in optical lattices where coherent control is achieved through laser cooling and spectroscopic techniques. Since the lattice geometry has an intrinsic massive parallelism, it proves to be an intriguing system for scalable, fault-tolerant quantum computation.

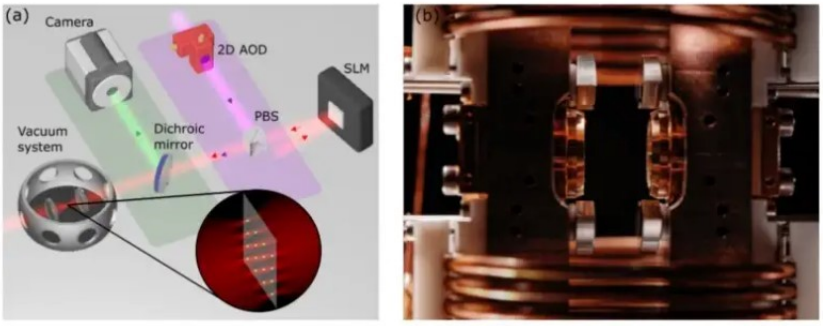



Figure 4.18: Overview of a neutral atom quantum computer

**Advantages:**

- Scalability - possible massive parallelism due to lattice geometry
- Long decoherence times (weak coupling with the environment)
- Availability of controlled interactions
- Well-developed experimental techniques for initialization, state manipulation, and readout

**Disadvantages:**

- Decoherence during the gate operations
- Unreliable lattice loading and individual addressing

**Quantum Memory:**

Requirements for choosing an atomic species and design of neutral atom trap:

- the intrinsic decoherence rate of the trap must be low
- the trap must provide confinement on a scale much smaller than the optical wavelength
- the trap must be compatible with the encoding of quantum information in an atomic internal and/or motional degree of freedom
- the interaction between atomic qubits must be precisely controlled and programable.

**Environment:** Here, the environment produced is in the form of optical lattices which are periodic arrays of micro-sized traps created by ac-Stark shift in the interference pattern of a set of intersecting laser beams. They serve as excellent traps for atomic species when they are detuned far from atomic resonance.

Based on this, we can consider 2 types of traps:

- Magnetic traps -

  These traps are based on the interaction between atom's permanent magnetic dipole moment and magnetic field portrayed as $-\mu \cdot B$. These traps have long coherence times (especially for BEC atomic vapours), but are difficult to encode and struggle to manipulate large numbers of atomic qubits at once.

- Optical traps -

  These traps are based on the interaction between an induced electric dipole moment and a laser field portrayed as $-d \cdot E/2$. They are intrinsically dissipative in nature due to photon scattering but their tremendous flexibility in designing enables high trapping potential through different atomic species and optical field parameters and thus are chosen widely. In large detuning, the optical potential can be calculated using perturbation theory, $U(x) = -\frac{|E_o(x)|^2}{4}\vec{\epsilon}(x) \cdot \vec{\alpha} \cdot \vec{epsilon}(x)$

**Quantum state:**

For the case of a quantum state, we can produce quantum gases based on bosons with integer spin or fermions with half-integer spin trapped in an optical lattice and can encode information in the internal ground hyperfine states of these neutral trapped atoms. For the selection of an atomic species, alkali atoms are commonly used due to their ease of being laser cooled and trapped. Common isotopes of Na, Rb, Cs have nuclear spin and hyperfine structure ground states as $nS_{1/2}(F = I \pm \frac{1}{2})$ and excited states as $nP_{1/2}(F = I \pm 1/2), nP_{3/2}(F = I \pm 1/2, 3/2), D1$ and $D2$ resonance lines.

Example: A linear polarized wave with $500W/cm^2$ forms a 1D optical lattice to trap a Cs atom whose excited state is tuned at 50 GHz D2 resonance line. THis vibrational level structure is highly resolved and allows the atom to undergo many thousand oscillations between spontaneous emission events.

For alkali atoms excited near the D2 resonance line, at a detuning much marger than the hyperfine splitting but less than the fine structure splitting in the excited state, the light shift can be cast in the form

$$\hat{U_F}(x) = U_J(x) + B_{eff}(x) \cdot \frac{\hat{F}}{F}$$

where

$$U_J(x) = \frac{2}{3}U_I|\vec{\epsilon_L}(x)|^2, B_{eff}(x) = -\frac{i}{3}U_I[\vec{\epsilon_L}(x)X\vec{\epsilon_L}(x)]$$

where $U_I$ is the single beam light shift

Moreover, 2D and 3D optical lattices can formed through a combination of standard laser cooling in a magneto-optic trap as

$$|1\rangle_{\pm} = |F_{\uparrow} = I + 1/2, M_F = \pm 1\rangle \otimes |\psi\rangle_{ext}$$
$$|0\rangle_{\pm} = |F_{\downarrow} = I - 1/2, M_F = \mp 1\rangle \otimes |\psi\rangle_{ext}$$

where $|\psi\rangle_{ext}$ represent the external motional quantum states

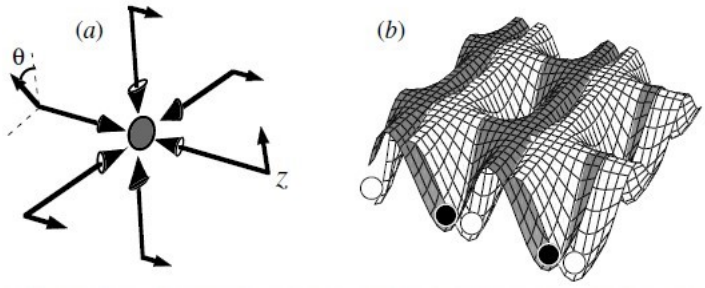



Figure 4.19: Schematic of a 3D blue-detuned optical lattice

Example: using cold atom physics, trapped neutral atoms like Cs in an optical lattice (laser beams forming energy wells) cooled to millionth of a kelvin gives the 2-level system as hyperfine energy levels of the atom (making use of ryberg atoms), controlled and entangled with lasers.

**Quantum CPUs:**

**Initialization:**

We understand that we need to prepare the internal state, done by putting atoms in the ground hyperfine state and then optical pumped into the optical lattice. Here, the motional states may be cooled to motional ground states and loading with one atom per site where a Mott insulator transition takes place. Achievement is either through adiabatic turn on by getting all the condensates in the lowest state, or non-adiabatically by the superposition of excited states. Though, since even a tightly focussed laser hits more than one atom, atoms in adjacent lattice sites are not optically resolved.

Trapping is done though laser cooling by doppler cooling in one dimension, or by magnetic trapping of quantum states whose magnetic or zeeman energy increases with increasing field and states when energy decreases, depending on the orientation of the moment compared to the field (magneto-optical trapping).

**Logic Operations:**

- Single-bit operations

  We understand that the atoms are trapped in a lattice and can be manipulated using light pulses. We see that the rotations of qubit vector or the change in the quantum state can be done using two laser beams which induce transitions between the atomic qubit states.

These rotations are caused by providing coherent Raman pulses and ac-Stark shifts where the rydberg state reaches an intermediary excited state and then comes back to the other state similar to an induced stimulation process.

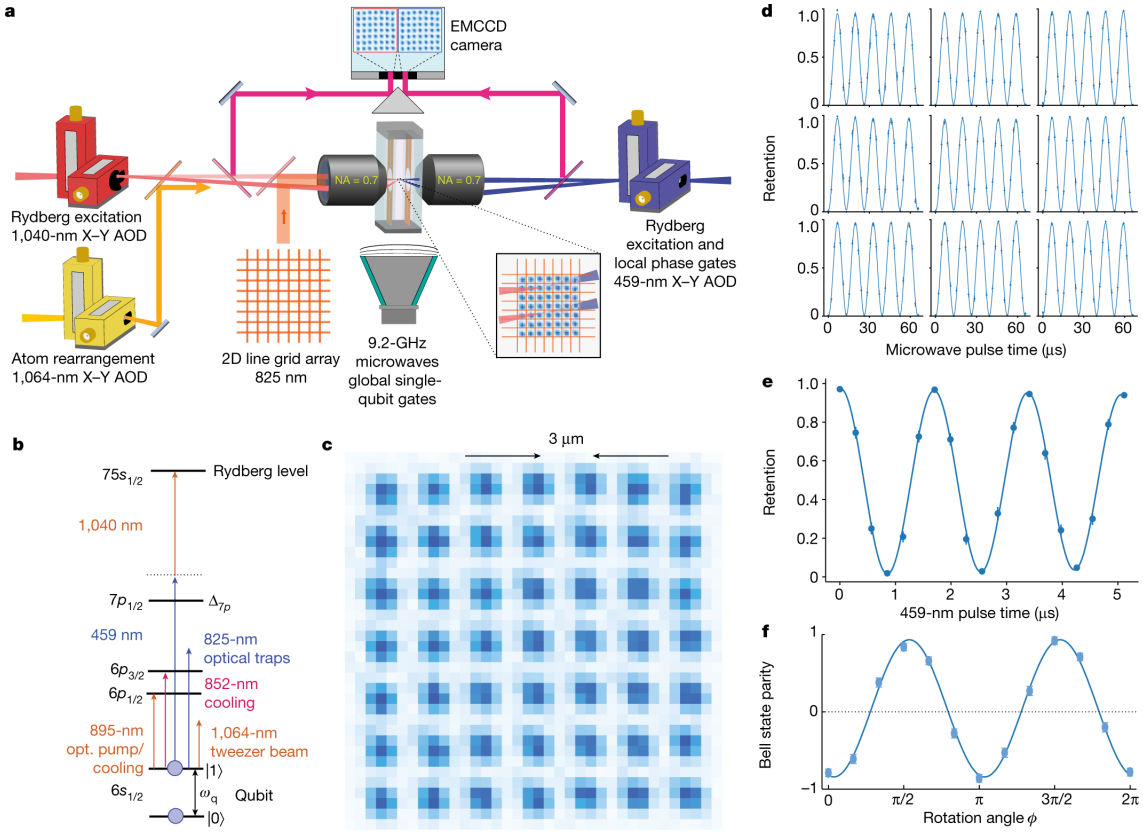



Figure 4.20: Detailed computation using neutral atoms

- Two-qubit quantum gates

  Since, we need an interaction between two trapped atoms, we find that there can be particular interactions which can form the basis for communication:

  electric-dipole interactions between atoms

  ground state elastic collisions

  magnetic-dipole interactions between pairs of atoms

  Considering the dipole-dipole interactions between the two atoms, we can form an effective hamiltonian for the atom-laser interaction, together with a dipole-dipole interaction as

$$H_{AL} = -\hbar(\Delta + i\frac{\Gamma}{2})(D_1^\dagger \cdot D_1 + D_2^\dagger \cdot D_2) - \frac{\hbar\Gamma}{2}(D_1^\dagger \cdot \vec{\epsilon_L}(r_1) + D_2^\dagger \cdot \vec{\epsilon_L}(r_2) + h.c.)$$

$$H_{dd} = V_{dd} - i\frac{\hbar\Gamma_{dd}}{2} = -\frac{\hbar\Gamma}{2}(D_2^\dagger \cdot \overleftrightarrow{T}(k_L r) \cdot D_1 + D_1^\dagger \cdot \overleftrightarrow{T}(k_L r) \cdot D_2)$$

  The performance of a quantum gate can be charaterized by a figure of merit that measures the ratio of the coherent interaction energy of two qubits to their collective decoherence rate.

Assuming that the strength of the excited dipole is independent of the internuclear coordinate separating the atoms, we can calculate the figure of merit for coherent dipole-dipole level shift as:

$$\kappa = \frac{\langle V_{dd} \rangle}{\langle \hbar \Gamma_{tot} \rangle} = \frac{-\hbar\Gamma \langle D_q^\dagger D_q \rangle_{int} \langle f_{qq} \rangle_{ext}}{2\hbar\Gamma \langle D_q^\dagger D_q \rangle_{int} (1 + \langle g_{qq} \rangle_{ext})} = \frac{-\langle f_{qq} \rangle_{ext}}{2(1 + \langle g_{qq} \rangle_{ext})}$$

which depends on geometry, external states and the direction of polarization and independent of the strength of the dipole.

Using these principles, the atoms are collided by merging wells which gives the possibility of inelastic collisions and we can formulate some basic gates as:

CPHASE gate

Here, we take into consideration ellipsoidal wells which produces an axially symmetric harmonic potential with two atoms in the vibrational ground state, and the figure of merit is

$$\kappa \approx -\frac{1}{4} \langle f_{00}(r, \theta) \rangle_{ext} = \frac{1}{16\sqrt{\pi}\eta_\perp^2 \eta_\parallel} [-2 - 3\frac{\eta^2}{\eta_\perp^2} + 3(\frac{\eta^3}{\eta_\perp^3} + \frac{\eta}{\eta_\perp}) \tan^{-1}(\frac{\eta_\perp}{\eta})]$$

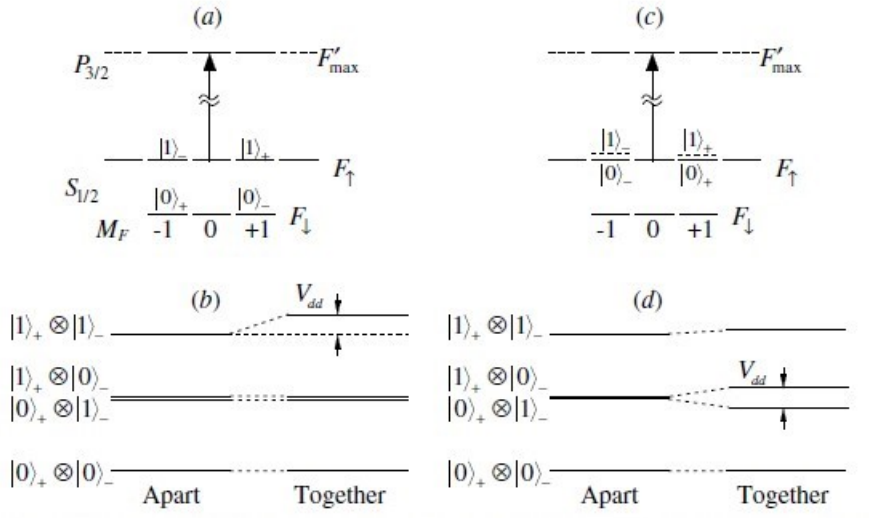



Figure 4.21: Energy level structure for CPHASE configuration

$\sqrt{SWAP}$ gate

Here, we approach this geometry as higher vibrational states of overlapping spherical wells and the figure of merit for this gate is

$$\kappa \approx -\frac{1}{4} \langle 1_+ 1_- | f_{00} | 1_+ 1_- \rangle = -\frac{1}{140\sqrt{\pi}\eta^3} \approx -\frac{4.02 \cdot 10^{-3}}{\eta^3}$$

**Relevant Work and Developments:**

Here, we mention all the major companies working in these superconducting quantum computers along with their public announcement of the recent number of qubits that they have successfully achieved for computation(even though that no of qubits doesnt tell us about the error rate or quantum volume).

| | |
|---|---|
| **ColdQuanta - 100** | **Atom Computing - 100** |
| **Pasqal (Simulator) - 200** | **Quera (Simulator) - 256** |

### 4.4.7 Other Approaches(not built that much but promising):

**Electron-on-Helium qubit**

[8] [20]

**Introduction:** Here, we build a two-dimensional network of electrons on the surface of liquid helium as qubits which have microwave orbital frequencies. As we operate an very cold temperatures, we observe quantum mechanical properties and can create condensates with electrons in the ground state, which can be excited with resonant microwave fields at frequencies $\sim 120$ GHz. Here, the gate operations are implemented by long-range Coulomb interaction between electrons and the measurement state is achieved by selective ionization of excited electrons from the helium surface.

One of the main challenges is the deformations on the helium surface which modify the image charge potential for Rydberg and orbital states, and decoherence caused due to emission of ripplons or phonons in the helium substrate, whereas the decay rate slower compared to qubit operations and thus, coherence time are good showing promise in this type of technology.

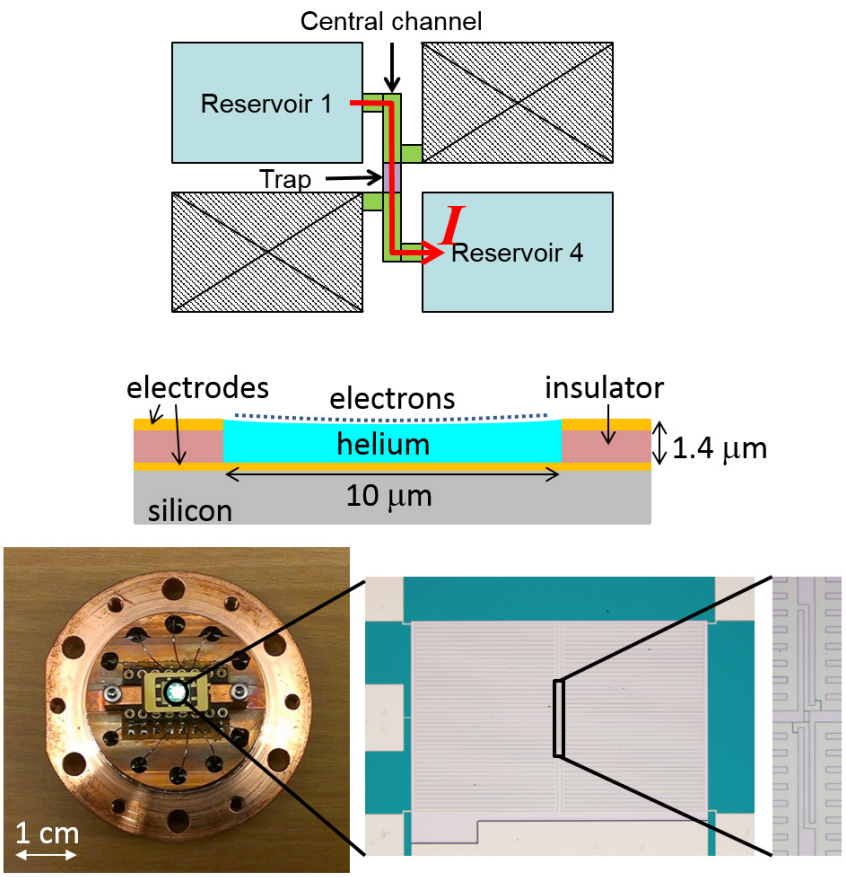



Figure 4.22: Representation of an electron-on-helium circuit

**Environment:** Our Circuit Quantum Electrodynamic devices consist of superconducting microwave resonators with an integrated electron-on-helium quantum dot. Here, the coplanar stripline resonator consists of two niobium center pins joined at one end and are situated below the ground plane at the bottom of a micro-channel($w = 3.5\mu m, d = 1.2\mu m, f_0 = 6.399GHz$, linewidth$k_{tot}/2\pi = 0.4MHz$) to deterministically populate the dot with N electrons. We partially unload the dot using the trap guard voltage to $V_{unlead} < 0$ which decreases the trap depth followed by a measurement of the resonator transmission at $(V_{trap}, V_{tg}) = (0.175, 0.0)V, T = 25mK$ and low incident microwave power ($n_{ph} \sim 5$) such that electrons respond linearly to the resonator's driving force.

**Qubit 2-level system:** The ground and excited Ryberg energy levels of electons form the basis states for these type of qubits. It is the quantized motional state/spin state of the electron trapped above the surface of liquid helium creating a 2d system on the interface of liquid helium and vacuum. Here, we now know that small electron clusters populate the quantum dot with N electrons sweeping the trap guard voltage to $V_{cluster} < 0$.

Here, the orbital frequencies of these clusters lie in the microwave regime and light-matter interactions are implemented using microwave photons and our concerned qubit is trapped in a potential well effectively as single electron-photon coupling strength - $g/2\pi = 4.8 \pm 0.3MHz$ which greatly exceeds the resonator linewidth - $k/2\pi = 0.5MHz$.

Anharmonicity is similar to that to that in superconducting qubits, indicating a reduced

linewidth and thus, the orbital state of a single electron on helium can be used as a qubit.

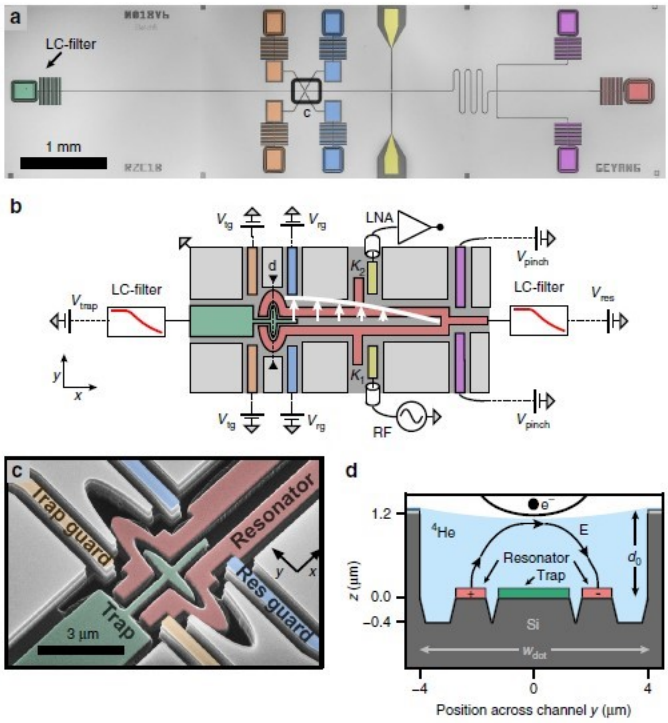



Figure 4.23: Electron-on-helium (a) optical micrograph (b) device schematic (c) scanning electron micrograph (d) schematic cross section

**Fabrication and Measurements:** Here, a 80 nm thick Nb ground plane is evaporated into a high resistivity ($> 10k\Omega cm$) Si $< 100 >$ wafer, followed by deposition of a 100 mm thick silicon oxide sacrificial layer(protection) and micro-channels are defined using a Raith EBPG-5000+ electron beam lithography system and etched using a $CHF_3/SF_6$ chemistry, followed by $HBr/O_2$ etch resonator center pins defined using e-beam lithography. After development, $150nm$ thick Nb layer evaporated and lifted-off, center pins remained on the bottom of the micro-channel.

[To improve robustness of the device and avoid electrical breakdown at low temperatures, we etch away an additional $\sim 400nm$ of Si substrate in between the resonator center pins. To this end, another layer of 80 nm thick $SiO_2$ deposited, and additional Si is etched. $SiO_2$ is removed using buffered HF and a deionized water rinse.]

Measurements are done using an Oxford triton 200 dilution refrigerator (base temperature 25 mK) where chip is mounted in a custom-designed hermitic sample cell and sealed with indium to prevent super fluid leaks. Helium supplied [liquid helium stable by surface tension] captures the electrons on the helium surface by thermal emmission from a tungsten filament above the chip, while applying a positive voltage to the resonator DC bias electrode ($V_{res} = 3.0V$) and a negative bias voltage to the filament. Now the electrons flow onto Nb ground plane and electron density $n \approx \frac{\epsilon_0 \epsilon_{He}}{e t_{He}} V_{res}^{th} = 9X10^{12} m^{-2}$ and the electrostatic potential near the dot approximated by

$$E/e = \alpha_0(V_{trap})x^2 + \alpha_1(V_{trap})y^2 + \alpha_2(V_{trap})y^4$$

**Example:** One prominent example for physically realizing this type of quantum computation is EEROQ by production of a single stable qubit, which can show promise in realizing practical quantum computation.

**Cavity Quantum Electrodynamics**

[27]

Now, a new method for computation arises from quantum experiments of trapping atoms and thus looks into the light-matter interactions at a microscopic level where quantum atomic states interact with optical cavities and their interaction is used for quantum communication. It presents a very flexible approach to quantum computing. In 2012, Nobel prize for Physics was awarded for the experimentation of controlling quantum system as a CQED interface between trapped ion and optical quantum communication atom (or molecule or quantum dot) in a resonant optical field. These microwave cavities with superconducting walls (perfect reflectors) houses Rydberg atoms which opened up a wide field of investigations for application in computing.

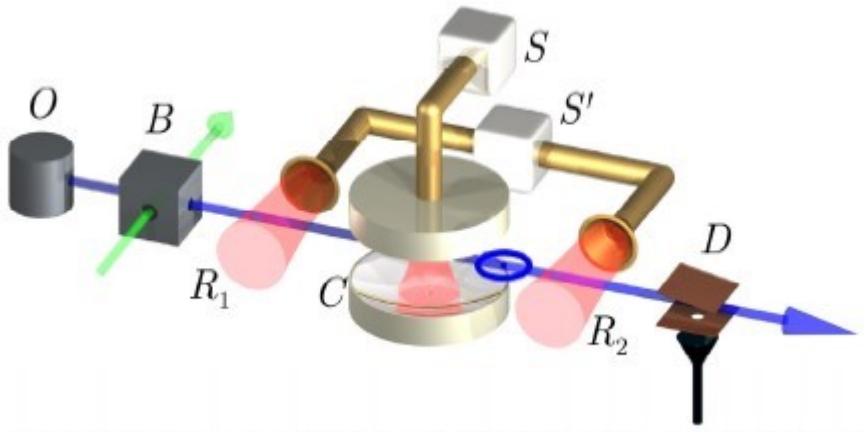



Figure 4.24: Circuit representation based on cavity quantum electrodynamics

Based on the interaction between light and matter, our quantum message can be interpreted in multiple ways:

- single photons in the dual rail representation as qubits
- photon states with atoms trapped in cavities providinig non-linear interactions between photons(necessary for entanglement)
- atoms in different states but communication through photons

There are 2 types of CQED computations setups:

| | **Microwave CQED** | **Optical CQED** |
|---|---|---|
| Quantum States | defined by the very excited "Rydberg" states interacting with superconducting millimeter-wave cavities | low-lying atomic levels interacting with room temperature optical cavities |

| | | |
|---|---|---|
| Advantage | very low dissipation rate and the pace of the atom-field entanglement process being slow giving high degree of control which can also lead to tailoring complex multi-qubit entangled states | interaction faster and faster dissipation (optical photons efficiently coupled in or out of the cavity) thus provides a natural and essential interface between flying photonic qubits for the transmission of quantum information and stationary atomic qubits for the storage of quantum information |
| Interaction | the energy is provided by excited atom entering the cavity and depositing a photon | atoms are in ground state and excitation of system through external laser |
| Photon Storage time | $1ms$ to $1s$ at few tens of Ghz frequencies using superconducting materials at cryogenic temperatures | 3 distinct time scales :- period of oscillatory exchange of single energy quantum between atom and cavity(Rabi time); transit time of atom through cavity; coupling of the combined atom-cavity system to the environment (photon lifetime in cavity and atomic lifetime due to spontaneous emmission) |
| Characteristics | high-field confinement for atom-field coupling with rydberg atom and alkali's valence electron promoted to large principal quantum number coupled with microwaves resulting in extremely long lifetime (30 ms for N = 50); also quantum entanglement manipulations realized by resonant atom-cavity interaction | for Z configurations, laser drives the atom which emits a photon into the cavity (short Rabi time in strong coupling regime), thus the laser excites the cavity where transmission modified by presence of atom and accurate knowledge of atom obtained by observing with unprecedented time resolution of the photons that escape through the mirror |

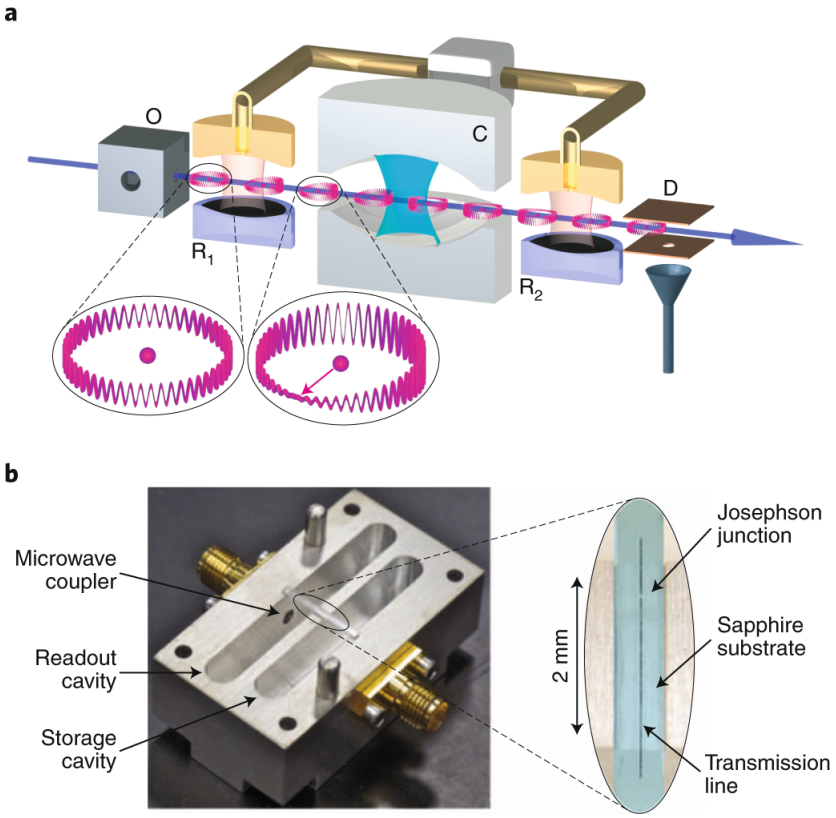



Figure 4.25: Physical example of a cqed circuit

We understand that it will be possible to repeatedly move trapped atoms in and out of the strong-coupling region in the near future enabling us to address individual or pairs of qubits of an atomic quantum register with a high-finesse cavity, thus this method can provide great flexibility

Moreover, developments show a lot of promise by blending atom-chip and CQED concepts and recent advances in nanotechnology allow for designing novel wavelength-sized optical cavities with photonic band gap materials and use of artificial atoms like quantum dots.

### Magnetic molecules or Molecular spins

[12]

This approach takes into account the nuclear spins of specific molecules or electronic spin in specific molecular structures and form a communication network based on molecular nanomagets manipulated by microwave pulses.

**Qubit:** Here, depending to our need, we can use the spin in the molecules as the quantum states, specfically nuclear spins of specific molecules for long coherence times, with scalability issues due to connection problem or electronic spins in specific molecular structures which can be coupled to superconducting resonators for communication.

Since the principle depends on magnetic spin, noise can caused by lattice vibrations, electric and magnetic noise, or any uncontrolled interaction of qubit with environment thermal vibrations, nuclear spins located on the ligands and solvent, or neighbouring electronic spins.

Considering these qubits as molecular nanomagnets, we establish a potential to run at 80 K as magnetic bistability is maintained even at these temperatures even though magnetic hysteresis is low to be practical. Examples include a molecular ring of $Cr_7NiF_6Piv_{16}$ with coherence time $1\mu s$ & $[V_{15}^{IV}As_6O_{42}(H_2O)]^{6-}$ with the same coherence time, while maximum coherence time of $700\mu s$ reached with $[V^{IV}(C_8S_8)]^{2-}$.

Even though the structure of the computing setup is still not yet settled, we can resort to coordination chemistry and/or supramolecular or even biochemical strategies:

- Electronic spin - This setup can be coupled to superconducting resonators for switchable to coherent communication channels between two different molecules
- Nuclear spin - Although this setup gives longer coherent times, it is not easy to connect thus providing diffciulty in scalability macroscopically.

  Thus, chemical design focuses on electronic interactions and to their coupling for specific devices.

We understand that the spins in solids or molecules act as discrete energy levels, manipulated by means of external electromagnetic fields and thus prove to be one of the simplest platforms to encode.

In 1990s, we observed d-block polynuclear molecular clusters show magnetic hysteresis at low temperatures and thus can be approximated to a giant anisotropic spin. Progressively, in 2000s, we see that f-block metal single magnetic ions can even portray magnetic bistability at room temperature or atleast liquid-nitrogen temperatures. Thus there is a lot of promise in lanthanide spin qubits trapped in molecules where control over the energy-level structure is done with the control over the crystal-field around the lanthanide ion and/or over the electro-nuclear hyperfine interactions.

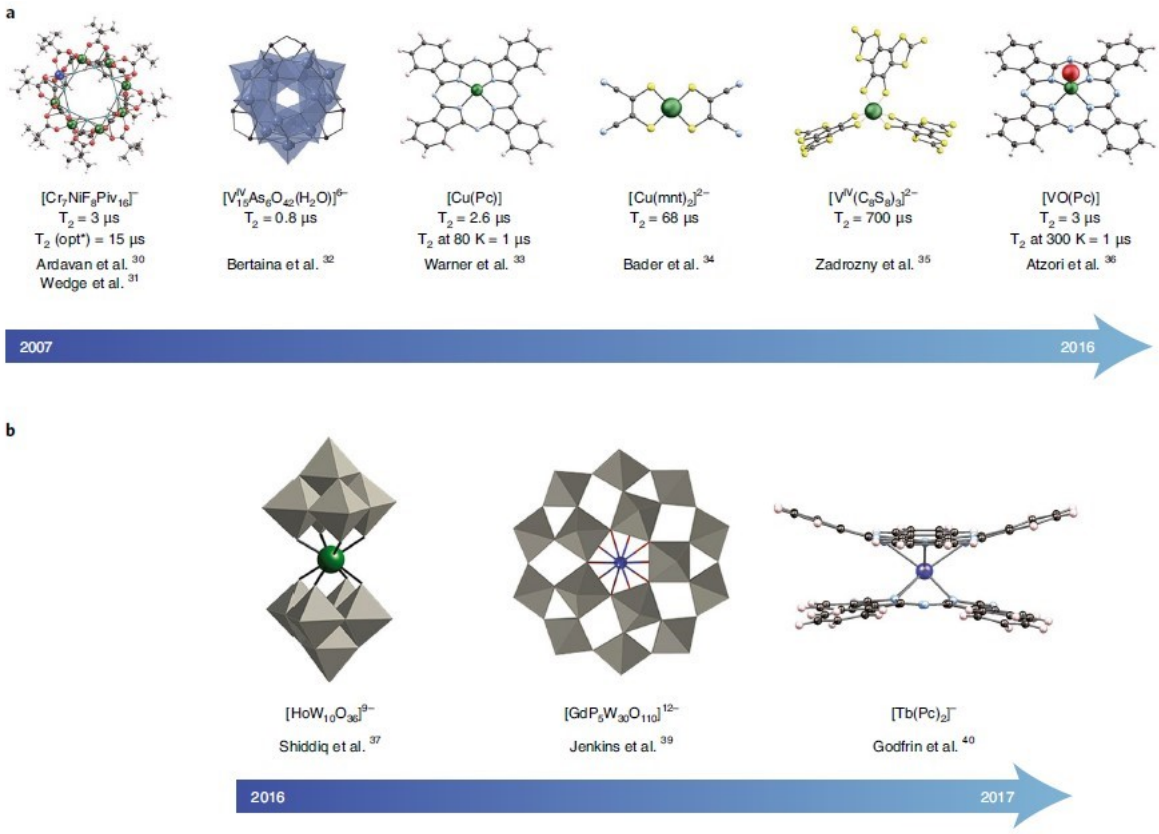



Figure 4.26: Some molecular complexes for spin qubits along with timeline

**Communication:** Here, the magnetic field adjusts the qubit energy for its manipulation with a resonant microwave pulse. We understand that the angular frequency of these oscillations(Rabi) using Lande factor, magnetic moment, angular momentum is given by

$$\Omega_R = \langle 0 | \, g_j \mu_B \hat{J} \cdot \vec{h_{m\omega}} \, | 1 \rangle \, / \hbar$$

We can implement the quantum gates by using the molecular dimers can host two spin qubits, like the dimers of $Cr_7Ni$ rings linked by redox active centers and transition metal clusters linked by photoswitchable dithienylethene units.

Thus, single qubit gates can be performed by resonant microwave pulses and SWAP and CNOT gates through binding two odd number of asymmetric $\beta$- diketone bridging ligands at two different coordination sites which can be triggered through microwave pulses and compatible transition frequencies giving them a significant edge over transition metals.

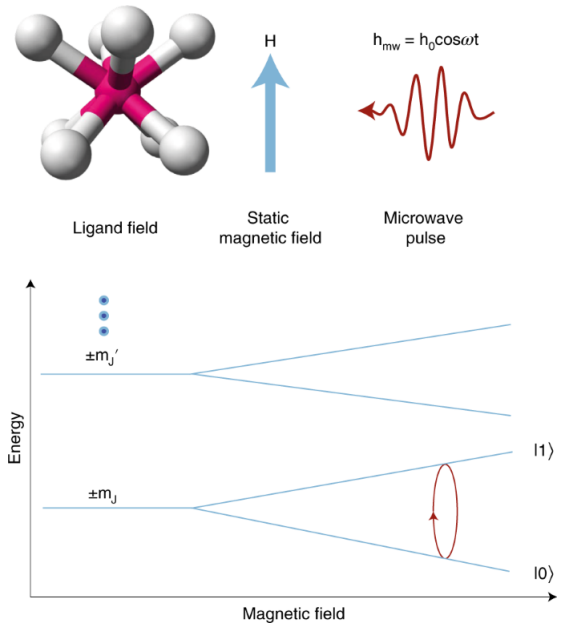



Figure 4.27: Representation of the spin energy levels

**Scope:** Moreover, we want to maximize quantum coherence to achieve non-trivial set of quantum operations in a minimum building block, for which this method shows a lot of promise as chemical design goes beyond molecular properties for further optimization which can enable scalability.

**Nuclear magnetic resonance Quatum computer(NMR)**

[18]

- This model delves into the aspect of studying the spin states of nucei within a molecule as the basic unit for quantum computation. These can be realized in either liquid state NMR(free qubits with an ensemble of molecules in a liquid sample) or solid state NMR(qubits in a nitrogen vacancy).
- Here, quantum states probed through the nuclear magnetic resonances and implementation as variation of nuclear magnetic resonance spectroscopy and thus is adopted by chemists mostly rather than physicists.
- Advantages include easy implemetation of arbitrary unitary transformations and great simplicity because of low energy scale and long time scale of radio frequency transitions, while the major disadvantage is the difficulty in implementing essential non-unitary operations.
- We also understand that the observed behaviour is dependent on the state of nuclear magnetic resonance quantum computer:

  Liquid state NMR - here, the atom's nuclei behave as spin-1/2 systems and inter-atomic bonds as interactions between qubits, and communication is through exploiting the spin-spin interactions to perform operations. When extrapolated, this concept is similar the trapped ions concept.

Solid state NMR - this is similar to a nitrogen vacancy diamond lattice, and thus have an advantage for the possibility to initialize the qubit and qubits to be localized precisely. Here, we can measure each qubit individually, and is lower temperature friendly for suppressing phonon decoherence.

- In general NMR computing, operations performed on the ensemble through radio frequency pulses applied perpendicular to a strong, static magnetic field, created by a very large magnet.

  The zeeman splitting creates splitting of a spectral line according the gyromagnetic ratio and the external magnetic field:

  $$\Delta E = \hbar \gamma B$$

  and the transitions are induced by an oscillating magnetic field with resonance frequency $\nu = \Delta E/h$ [Larmor frequency]

- While studying the NMR spectra, we find that the groups of peak splits (multiplets) indicate coupling between spins and the direct coupling between pairs of magnetic dipoles is represented as:

  $$D_{ij} \propto \frac{3\cos^2\theta_{ij} - 1}{r_{ij}^3}$$

  where a pure state is represented as $|\psi\rangle\langle\psi| = \frac{1}{2}(1 + \gamma_x\sigma_x + \gamma_y\sigma_y + \gamma_z\sigma_z)$ represented by Boltzamann formula for initialization of an isolated nuclear spin at thermal equilibrium

  $$\rho = exp(-\hbar\omega_I I_z/kT)/Tr[exp(-\hbar\omega_I I_z/kT)] = \approx \frac{1}{2}E - \hbar\omega_I I_z/kT$$

  where the first term is the maximally mixed state and unaffected by unitary evolution. So by removing constants, the thermal state can simply be described by $I_z$ and excitation is due to a magnetic field $B_1$ at a rate $\omega_1 = \gamma B_1$ and $\theta = \omega_1 t$

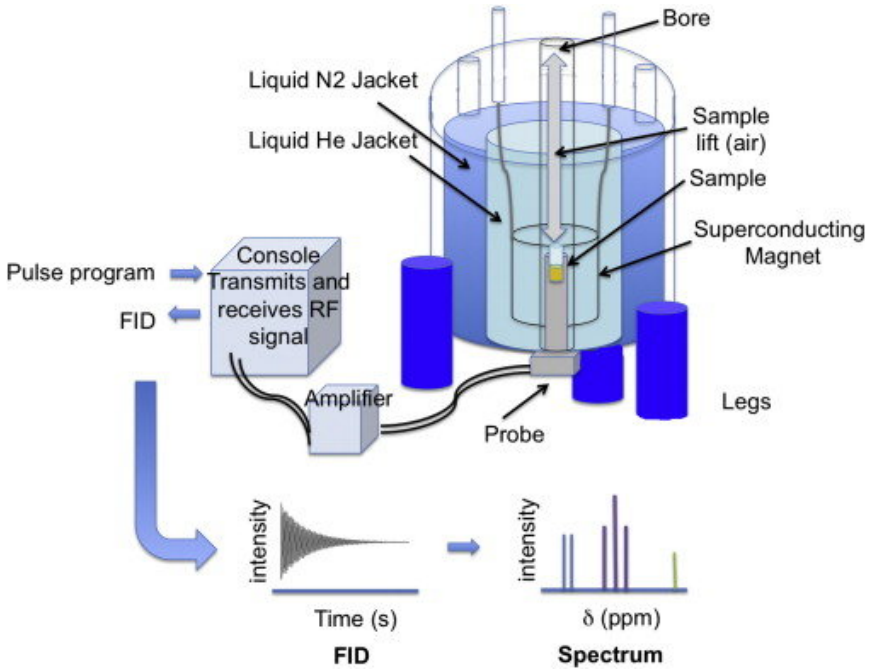



Figure 4.28: Representation of an NMR approach

- Moreover, the spin echo allows magnetisation free precession at the Larmor frequency and thus complex pulse sequences can be built up by combining spin echoes with selective and hard pulses.

- The quantum logic gates are built by designing conventional NMR pulse sequences:

  Single qubit gates:-

  The rotations of spin about axis using resonant RF pulses along the z-direction; and reference frame rotations for other dimensions.

  Two-qubit gates:-

  We find that the ising coupling Hamiltonian achieved using a homonuclear spin echo and J-couplings always active unless disabled.

- Thus, we see NMR computing shows promise as arbitrary unitary transformation can be implemented, and there is great experimental simplicity arising from the low energy scale and long time scale of radio frequency transitions, even though there is great difficulty in implementing essential non-unitary operations.

### 4.4.8 Non-hardware based realizations

Here, we would like to point out that there are many realizations of a quantum interaction of qubits through classical computers via quantum simulations. While there are companies like Google and IBM provide public access for their quantum computers to run quantum programs, these companies and many others build quantum simulators on classical computers. Since there is a need to understand quantum computations, there are many software based realizations of a problem solved through a quantum behaviour by creating quantum gates on a classical computer.

The most prominent software packages in the public eye delving into this aspect are:

| | | |
|---|---|---|
| **Qiskit - IBM** | **Pyquil - Rigetti** | **Cirq - Google Quantum AI** |
| *Q#* **- Microsoft** | **Pennylane - Xanadu** | |

Moreover, there are many other companies which can referred to as Non-hardware quantum companies with focus on software tools, research and applications:

| | | | |
|---|---|---|---|
| **Quantinuum** | **Riverlane** | **Multiverse Computing** | **Zapata Computing** |
| **1qubit** | **Qunasys** | **Q-Ctrl** | **QC ware** |
| **Heisenberg quantum simulations** | **Blueqat** | **Qsimulte** | **Entropica labs** |
| **Baidu** | **Phasecraft** | **Keysift Q** | **Strangeworks** |
| **QU & Co** | **Qubitor Labs** | **Atos** | **Classiq** |
| **Horizon** | **Parity QC** | | |

# Chapter 5

# Conclusion

Here, we discussed about the "mytery of quantum computers" where we described the area of quantum physics and how we apply it in physical terms in the

While discussing about the applications of quantum computing, we can establish the 10 immediate applications at the forefront of quantum computation which are:

- cybersecurity
- drug development
- financial modelling
- better batteries
- cleaner fertilization
- traffic optimization
- weather forecasting and climate change
- artificial intelligence
- solar capture
- electronic materials discovery

## 5.1 Some significant achievements in quantum computing

Now that we have described a little about quantum computing and its potential applications in different fields, we would like to point out the recent significant achievements paving way for implementing in quantum computing.

With the advent of a new era of computations and learning about the possible opportunities that can be taken advantage of, we can highlight some of the significant achievements accomplished till now:

- The photon triplets were formed by firing laser light into an atomic gas showing promise for solid state quantum computers. Also, in 2013, MIT & Harvard prepared pairs of photons to stick together using a weak laser beam through an ultracold gas of atoms resulting in the formation of a rydberg polariton in the atomic gas (just like highly excited electron shared by

several atoms). This was further developed in 2018 as both pairs and triplets of photons were formed from atomic gas resulting in a highly entangled state (photon triplets more strongly bound).

- In terms of quantum computing, latest advances reveal:

  Morello Autralian team created an accurate(99.96 percent accuracy) 1 qubit gate in a silicon quantum dot companies with Honeywell and other companies. They saw one-qubit operation fidelity up to 99.95%, two-qubit fidelity of 99.37% and a three qubit system comprising an electron and two phosphorous atoms, introduced in silicon via ion implantation which preserves quantum information in silicon for 35 seconds, due to extreme isolation of nuclear spins from their environment, but this makes interaction too difficult.

  Delft Netherlands created 1-qubit gates with 99.87% fidelity, 2-qubit gates with 99.65% fidelity using electron spins in quantum dots formed in a stack of silicon and silicon-germanium alloy.

  RIKEN team Japan developed 1-qubit gates with 99.84% fidelity, 2-qubit gates with 99.51% fidelity for a two-electron system using Si/SiGe quantum dots.

- Google has created their 72 bit quantum computer using quantum dots method which is mostly used for error correction. As they declared quantum supremacy, we have already discussed the major achievements of their approach, but can include their revolutionary creation of a true random number as the exact observation of the states and quantum gates cannot be done without changing the result according to quantum mechanics.

- Creation of a Time Crystal - Google collaborated with researchers to create a new state of matter where an array of qubits flip their state periodically in time driver by a laser but not absorbing any energy from the laser.

  According to the Watanabe-Oshikawa "no-go" statement, quantum crystals in equilibrium are not possible since it basically creates perpetual motion in the form of wilczek time crystal. So, we have expanded the definition of a time crystal in the form of a floquet time crystal where the quantum state goes back and forth only when driven by an external force. So the array of qubits flip their state periodically in time driven by a laser but not absorbing any energy from the laser.

  Also, it was realized that the Sycamore's qubits are ideal for time crystals where 20 qubits of superconducting aluminum with two possible energy states (each either up or down) set up arbitrarily and the interaction strenth between the qubits randomized so that interference can cause them to lock themselves in their assigned orientation. It was observed that when microwave radiation put onto them, their spins oscillated back and forth but the system didn't absorb or dissipate any net energy and entropy remained same (evading the second law of thermodynamics for ms that the time crystal lasted). This has applications in data storage, and can be used as a benchmark test for quantum computer's level of control.

- Quantum Cryptography -

  With the practical realization of Shor's algorithm, we realized that RSA encryption(the most widely used encryption method where the key is produced by multiplying two large prime numbers) becomes obsolete, and we can also see that quantum computers have the potential to make other classical encryptions obolete as well. Thus, we need a new method of encryption before a practical commercial quantum computer is built and this approach gives rise to

quantum key distribution. Here, we have created quantum protocols to create a secure private key and also presently have a quantum satellite Micius for satellite quantum key distribution.

- Quantum AI -

  With developments in machine learning and artificial intelligence, we see the potential of applying quantum computing in the field of Artificial Intelligence as it deals with large amount of data and computations can be made much more efficient using qubits. With applications in all areas of interest from finance to academics to retail, quantum computations can revolutionize the whole world through an exponential kind of computing as it computes multiple bits at the same time, for which two of the world's most prominent open source quantum AIs are Cirq and Qiskit by Google and IBM which allows people from around the world to understand quantum computing and build a framework upon which practical quantum computing can work.

- One of the the direct applications of quantum computers right now are quantum simulations used for solving complex and probabilistic equations in Chemistry & Physics. The examples include simulation of a simplified version of the energy state of a molecule consisting of 12 hydrogen atoms, with each of the 12 qubits representing one atom's single electron, or modeling a chemical reaction in a molecule containing hydrogen and nitrogen atoms, including how that molecule's electronic structure would change when its hydrogen atoms shifted from one side to the other. Since the energy of electrons dictates how fast a reaction occurs at a given temperature or concentration of different molecules, such simulations could help chemists understand exactly how that reaction works and how it would change if they altered the temperature or the chemical cocktail. Moreover, working with Bose Einstein codensates and the light-matter interactions, there are multiple phyhsical observations like superradiance, and a direct application might be getting the probabilistic curves of fermionic and bosonic interactions.

- Quantum artificial life in an IBM Quantum Computer is one of the most outstanding applications where quantum biomimetic protocol encodes tailored quantum behaviours belonging to living systems, like self-replication, mutation, interactions between individuals, and death, into the cloud quantum computer IBM ibmqx4 and entanglement spreads through generations of individuals, where genuine quantum information features are inherited through genealogical networks.

  A quantum router was also designed using a 5-qubit quantum processor "ibmqx4" which demonstrated two operations, i.e. entanglement generation between the control qubit and the signal paths, and the preservation of signal information after the routing process. It was also verified for a 3-qubit and 1-qubit quantum state tomographically.

## 5.2 Future plans

| Company (error corrected qubits) | Current qubits | Goal |
|---|---|---|
| IBM(2) | 127 | 2023-433 qubits<br>2024 - 1121 qubits<br>2026 - 1 million + qubits |
| Google(3) | 53 | 2030 - 1 million qubits |

| | | |
|---|---|---|
| D-wave(4) | quantum annealing chip 5760 qubits, not universal but 2025 - 7000 qubits with universal gates | |
| Rigetti(6) | 80 | 2024- 1000 qubits<br>2026 - 4000 qubits |
| Psiquantum(7) | optical quantum computers | 100s of logical qubits and billions of gates by 2025 |
| ColdQuanta(8) | atoms and optical tweezers give 100 qubits | 2024-1000 qubits |
| QONQ(17) - detailed | 32 | 2022-25 then 29, 35, 64, 256, 384, 1024 - algorithmic qubits |
| Pasqal(18) | simulated 200 bits | 2023-1000 practical qubits |
| Quera(19) | simulated 256 bits | practical 64 qubits by 2024<br>1024 qubits by 2025 |
| Silicon Quantum Computing(20) | 10 qubits by 2024<br>100 error corrected qubits by 2030 | |

With this information, we can say with much confidence that if these companies hold true to their goals, quantum computers can have practical applications in about 5 years which can revolutionize all aspects of technology as we perform an indirect way of computation using quantum mechanics.

# Bibliography


[1] Scott Aaronson. "BQP and the polynomial hierarchy". In: *Proceedings of the forty-second ACM symposium on Theory of computing*. 2010, pp. 141–150.

[2] Janusz Adamowski, Stanis law Bednarek, and Bart lomiej Szafran. "Quantum Computing with Quantum Dots". In: *Schedae Informaticae* 14 (2005).

[3] Andris Ambainis. *Quantum algorithms for formula evaluation*. 2010.

[4] Priyadharshini Balasubramanian et al. "Discovery of ST1 centers in natural diamond". In: *Nanophotonics* 8.11 (2019), pp. 1993–2002.

[5] Gilles Brassard, Peter Høyer, and Alain Tapp. "Quantum counting". In: *International Colloquium on Automata, Languages, and Programming*. Springer. 1998, pp. 820–831.

[6] Colin D Bruzewicz et al. "Trapped-ion quantum computing: Progress and challenges". In: *Applied Physics Reviews* 6.2 (2019), p. 021314.

[7] Iulia Buluta and Franco Nori. "Quantum simulators". In: *Science* 326.5949 (2009), pp. 108–111.

[8] AJ Dahm et al. "Using electrons on liquid helium for quantum computing". In: *Journal of low temperature physics* 126.1 (2002), pp. 709–718.

[9] David Deutsch and Richard Jozsa. "Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), pp. 553–558.

[10] Ivan H Deutsch, Gavin K Brennen, and Poul S Jessen. "Quantum computing with neutral atoms in an optical lattice". In: *Fortschritte der Physik: Progress of Physics* 48.9-11 (2000), pp. 925–943.

[11] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. "A quantum approximate optimization algorithm". In: *arXiv preprint arXiv:1411.4028* (2014).

[12] Alejandro Gaita-Ariño et al. "Molecular spins for quantum computation". In: *Nature chemistry* 11.4 (2019), pp. 301–309.

[13] Bryan T Gard et al. "An introduction to boson-sampling". In: *From atomic to mesoscale: The role of quantum coherence in systems of various complexities*. World Scientific, 2015, pp. 167–192.

[14] Robin Gaudreau and David Ledvinka. "Knot theory and quantum computing". In: *arXiv preprint arXiv:1901.03186* (2019).

[15] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. "Quantum algorithm for linear systems of equations". In: *Physical review letters* 103.15 (2009), p. 150502.

[16] Loıc Henriet et al. "Quantum computing with neutral atoms". In: *Quantum* 4 (2020), p. 327.

[17] He-Liang Huang et al. “Superconducting quantum computing: a review”. In: *Science China Information Sciences* 63.8 (2020), pp. 1–32.

[18] JA Jones. “Nuclear magnetic resonance quantum computation”. In: *Les Houches*. Vol. 79. Elsevier, 2004, pp. 357–400.

[19] Pieter Kok et al. “Linear optical quantum computing with photonic qubits”. In: *Reviews of modern physics* 79.1 (2007), p. 135.

[20] Gerwin Koolstra, Ge Yang, and David I Schuster. “Coupling a single electron on superfluid helium to a superconducting resonator”. In: *Nature communications* 10.1 (2019), pp. 1–7.

[21] Carlile Lavor, LRU Manssur, and Renato Portugal. “Grover’s algorithm: Quantum database search”. In: *arXiv preprint quant-ph/0301079* (2003).

[22] Frédéric Magniez, Miklos Santha, and Mario Szegedy. “Quantum algorithms for the triangle problem”. In: *SIAM Journal on Computing* 37.2 (2007), pp. 413–424.

[23] Koji Nagata et al. “A generalization of the Bernstein-Vazirani algorithm”. In: *MOJ Ecol. Environ. Sci.* 2.1 (2017), p. 00010.

[24] Jeremy L O’brien. “Optical quantum computing”. In: *Science* 318.5856 (2007), pp. 1567–1570.

[25] Sébastien Pezzagna and Jan Meijer. “Quantum computer based on color centers in diamond”. In: *Applied Physics Reviews* 8.1 (2021), p. 011308.

[26] Renato Portugal. “Element distinctness revisited”. In: *Quantum Information Processing* 17.7 (2018), pp. 1–15.

[27] Jean-Michel Raimond and Gerhard Rempe. “Cavity Quantum Electrodynamics: Quantum Information Processing with Atoms and Photons”. In: *Quantum Information: From Foundations to Quantum Technology Applications* (2016), pp. 669–689.

[28] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. “An introduction to quantum machine learning”. In: *Contemporary Physics* 56.2 (2015), pp. 172–185.

[29] Peter W Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[30] Daniel R Simon. “On the power of quantum computation”. In: *SIAM journal on computing* 26.5 (1997), pp. 1474–1483.

[31] Scott E Smart and David A Mazziotti. “Quantum solver of contracted eigenvalue equations for scalable molecular simulations on quantum computing devices”. In: *Physical Review Letters* 126.7 (2021), p. 070504.

[32] Jules Tilly et al. “The variational quantum eigensolver: a review of methods and best practices”. In: *Physics Reports* 986 (2022), pp. 1–128.

[33] Hristo S Tonchev and Nikolay V Vitanov. “Quantum phase estimation and quantum counting with qudits”. In: *Physical Review A* 94.4 (2016), p. 042307.

[34] Wim Van Dam and Gadiel Seroussi. “Efficient quantum algorithms for estimating gauss sums”. In: *arXiv preprint quant-ph/0207131* (2002).

[35] Frédéric Wang. “The hidden subgroup problem”. In: *arXiv preprint arXiv:1008.0010* (2010).