Quantum Computing Internship Final Report
Jacobs University Bremen

15.06.2021-15.08.2021

Sudip KC, Nitesh Khatiwada

Supevisor: Prof. Peter Schupp

October 31, 2021

1 Introduction

Since Newtonian mechanics emerges as a special limit of quantum mechanics, quantum mechanics can only have greater computational power than classical ones. The great pioneers and visionaries who pointed the way towards quantum computer, Deutsch, Feynman, and others were stimulated by such thoughts. The significant progress in the field has been made since then with today's major tech companies like Google, IBM, Microsoft and different Government Agencies are trying to achieve the state of quantum supremacy –term coined by John Preskill describing the immense computational ability of a quantum computer to solve a problem that no classical computer can do it in any feasible amount of time.
Qubit is the building block of quantum computer, and unlike in classical computer where electron's flow determines the bit's value $(0 \text{ or } 1)$, the particle's spin determines the state of the qubit. Hence, the control of quantum properties of the particles are essential to build a qubit. Qubit design determines the performance speed, coherence time and controllability of the today's system. The characteristics of the quantum hardware follows the following "DiVincenzo criteria [1]".

1. A scalable physical system with well characterized qubit.
2. The ability to initialize the state of the qubits to a simple fiducial state.
3. Long relevant decoherence times.
4. A "universal" set of quantum gates.
5. A qubit-specific measurement capability.

2 State of the art in Hardware Architecture

The different types of qubits have been realized to use for quantum computing, some of them are discussed here with their pros and cons.

A. Superconducting Qubits
Superconducting Qubits generally use Josephson junction , a thin insulating barrier between two superconductors, at extremely low temperature (achievable using $^3He/^4He$ dilution refrigerators), due to which they exhibit quantized energy levels (due to quantized state of electronic charge or magnetic flux). The two lowest states can be accessed selectively to realize the qubit. The Josephson junction makes the energy difference between its levels distinct, and this difference may be uniquely addressed by a frequency f_{01}. This means that microwave radiation tuned at a certain frequency causes transitions between these two states without accessing the higher-excited states–a realization of two level quantum system.

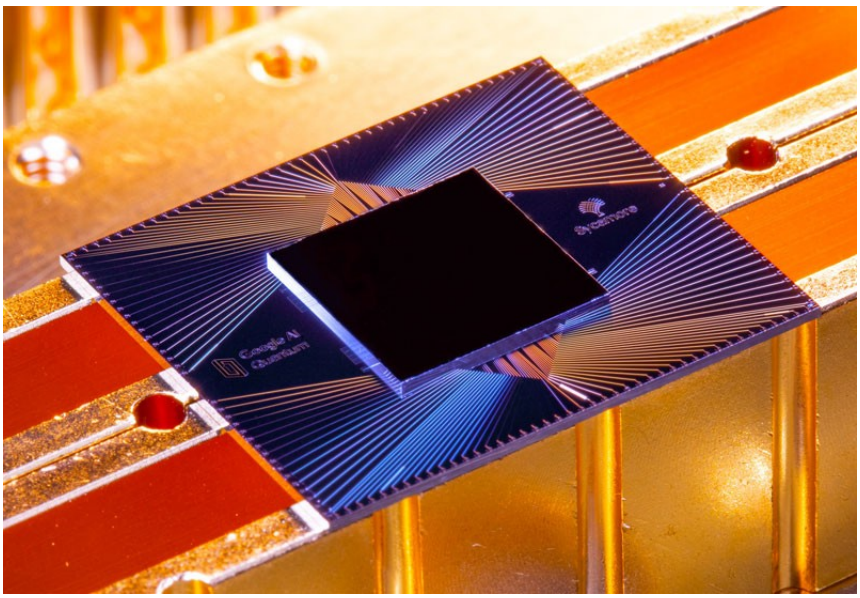


Figure 1: The Sycamore chip is composed of 54 qubits, each made of superconducting loops.
Credit: Erik Lucero at Google

The increase in number of qubits decreases the fidelity or "closeness" of two quantum states [2], and has been a major obstacle to build scalable quantum computer with superconducting qubits.

Dispersive readout and High-fidelity single-shot readout are today's common techniques implemented in measurement of the result of quantum computation. Dispersive readout obtains the qubit state information through the readout resonator. The qubit circuit is coupled to the readout resonator through capacitance or inductance, and the state of the qubit is detected by measuring the transmission coefficient of the readout resonator. High-fidelity single-shot suppresses spontaneous emission and uses Josephson effect to amplify the output signal [3].

More on Josephson Junction
When a material becomes superconducting, the electrons form Cooper pairs (formed by two electrons linked together, the speed of which are opposed and the spins of which are head-to-tail) and condensate in the shape of unique collective quantum wave. If the electric insulator separating the two superconductors is very thin (only a few nm), then the wave can somehow spill out of the superconductor which enables the electron pairs to go through the insulator due to a quantum effect called tunneling effect. When spontaneously going from one superconductor to another, the pairs create an electric current. Each superconductor is characterized by a quantity called phase, with a subtle signification. The electric current in the junction is a continuous current, the value of which is proportional to the sine of the phase difference between the two superconductors.

B. Trapped Ion Qubits

Individual ions serve as qubits. Atomic ions are trapped in space using electromagnetic fields in vacuum to avoid interactions with background molecules in the environment. Most trapped ion quantum computing systems use a Paul trap (time-dependent electric field), where a radio frequency (RF) signal is applied to two electrodes arranged in parallel to ground electrodes to form a quadrupole RF field (Figure 2.b). At the quadrupole "null"–where the RF field vanished–atomic ions feel a trapping potential, which typically takes the shape of a line (Figure 2.a). Each ion in the chain interacts with every other ion in the chain due to the strong Coulomb interaction in a tight trap through motional degree of freedom that is shared among the ions. This interaction can be leveraged to realize quantum logic gates between non-adjacent ions, leading to dense connectivity among the qubits in a single ion chain [2].

Qubit measurement is carried out by "state-dependent fluorescence". The ion is illuminated with a laser beam that causes only one of the two possible output states to scatter photons repeatedly, which can be measured with an optical detector. The presence/absence determines the state of the qubit [4].

Trapped ions are easier to scale, but consequently the meaningful control over individual ions is lost.

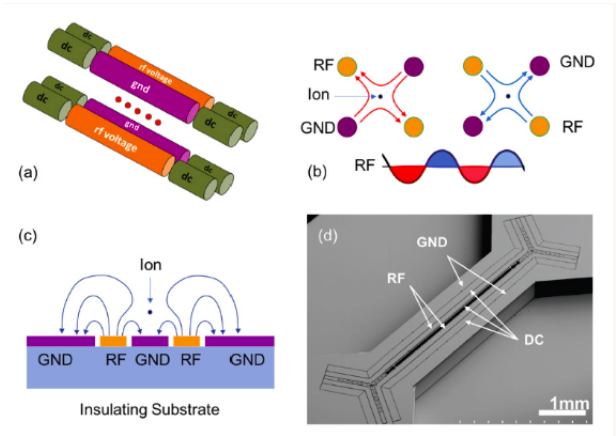


Figure 2: Operating principle of RF Paul trap. (a) An example of a traditional RF Paul trap using four rods. Two rods in the diagonal serve as RF grounds, while an RF voltage is applied to the remaining two. This geometry creates a quadrupole electric field profile in the plane perpendicular to the axis of the rods and forms a one-dimensional (1D) linear trapping potential, where a chain of ions can be readily trapped. (b) During the negative cycle of the RF voltage (red arrows), the positively charged ion is pushed away from the ground electrodes toward the RF electrodes, while during the positive cycle of the RF voltage (blue arrows), the ions are pushed in the opposite direction. If the frequency of the RF voltage is much higher than the natural motional frequency of the ion (called the "secular frequency"), then the ions feel confining potential where the electric field forms a quadrupole null ("zero-field region"). (c) A linear trapping potential can be created by electrodes fabricated on a planar surface of a substrate. The cross-sectional view of the electric field forms the quadrupole null, and a linear trap is formed above the surface of the trap. (d) An example of a microfabricated surface trap, designed to provide adequate optical access to the ions trapped above the surface of the trapping electrodes.
Credit: (a) Image from D. Hayes, Ph.D. thesis, University of Maryland, 2012. (b, d) Image from Quantum Computing: Progress and Prospects, The National Academic Press, 2019. (c) Image courtesy of Sandia National Laboratories, 2015

C. Photonic Quantum Computation

The qubits are the photons with two different polarizations. The weak interaction property of photon allows relatively larger coherence time; thus, long distance quantum communication could be effective with photonic qubits. However, weak interaction property also makes it difficult for entanglement, and multi-qubits system are not properly feasible. Additionally, the problem of photon loss (equivalently information loss) and phase errors are also routine in Photonic Quantum Computation. The weak interaction problem can be largely overcome with using non linear devices into the quantum network, but this is a difficult task. This has been recently solved using solely linear optical tools, single photon sources and photon detectors[5]. Photon loss has been dealt with using stabilizer code. Stabilizer codes are eigenspaces of commutative groups consisting of Pauli operators. If any one qubit of the code is not measured, all the measured ones can be recovered by adapting the recovery procedure so that the surviving qubit is teleported together with the measured ones using an entanglement modified by projecting suitable operators [6]. Additionally, the steady source of suitably initialized photons is needed for the computation due to quantum gates being probabilistic. Analyzing all these limitations of this method, it seems highly unlikely to scale with current understanding.
However, we cannot discard the ultimate scalability of Photonic Quantum Computation. Since the photons used in photonic quantum computing typically have wavelengths that are around a micron, and because the photons travel at the speed of light and are typically routed along one dimension of the optical chip, the number of photons, and hence the number of qubits, in a photonic device cannot be made as large as in systems with qubits that can be localized in space. However, arrays with many thousands of qubits are expected to be possible. [2]

D. Semiconductor Qubits

Semiconductor qubits can be either optically or electrically controlled. Semiconductor qubits can be either optically or electrically controlled [2].

- Optically gated: These semiconductor qubits use optically active defects or quantum dots that induce strong effective coupling between photons. Two-qubit gates between these qubits either requires them to be extremely close together (tens of nanometers), which makes optical addressing

of the detects extremely hard, or requires them to be coupled using photons, which makes the interaction weak and entanglement generating gates tend to be slow. This complicates to create scalable system. On the other hand using quantum dots, which couple strongly with photons, makes it possible to create high-fidelity photon-mediated gates. Since qubits speeds are also high, decoherence would also be high. Additionally, optical properties of quantum dots depend on its shape and size, thus uniform and predictable quantum dot sizes are critical.

- Electrically gated: These qubits use voltage applied to lithographically defined metal gates to confine and manipulate the electrons that form the qubits. Thus, in principal, such qubits have the potential for scalability to billions of qubits because the methods used for fabrication are very similar to those used for classical electrons and the qubit footprints are substantially less than square micron. The current challenge for the field is the development of reliable and high fidelity two qubit gates because of decoherence due to charge noise. Also, because of similarities in the cooling requirements, the control strategies and the frequency range of the qubit control voltages with those of superconducting qubits, it will be necessary to overcome crosstalk and fanout issues similar to those faced by superconducting qubits. These issues will be especially challenging in this system, since the small spacing between the qubits will exacerbate the coupling between wires, and it will be harder to create scalable control/measurement layers that can interface with the qubits.

E. Topological Qubits

The main motivation to develop topological qubits is less problem to deal with error correction. Topological quantum computation enables operations on the physical qubits to have extremely high fidelities because the qubit operations are protected by topological symmetry implemented at the microscopic level. However, implementation of topological quantum computation is found to be extremely challenging. The arrays of nanowires of a material with strong spin-orbit coupling should be strongly coupled to superconducting films, where the single-particle excitations are highly suppressed. Some of the complexities that must be dealt with are that the excitations on the superconducting nanowires are measured via coupling to non-superconducting quantum dots, and the couplings between these dissimilar systems must be well controlled and tunable to implement the necessary operations [2].

F. Optical Lattice

Optical Lattices are formed by counter propagating lasers producing standing electromagnetic waves creating a spatially periodic polarization pattern. The resulting periodic potential may trap neutral atoms via the Stark shift. Using optical lattices, one can control to an unprecedented degree the environment in which the atoms sit. For example, one can produce one, two, and three dimensions with a wide variety of lattice spacing and structures in which the neutral atoms can be trapped as show in Fig 3. As the lattices becomes deeper, more exotic condensed matter behaviour kicks in. One can convert

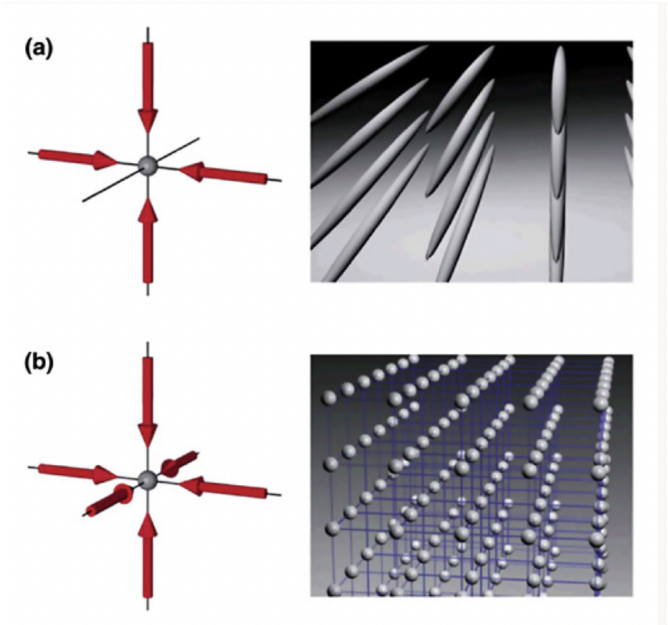


Figure 3: The left hand panels show laser configurations forming (a) two- and (b) three- dimensional potentials. The right hand panels are schematics of corresponding arrays of neutral atoms that can be trapped by these potentials. SOURCS: I.Bloch, Johannes Gutenberg University, Mainz Germany.

from a superconducting state, where atoms are delocalised over the whole lattice much like electrons in a superconductor, to a so called Mott insulator state. In the latter state, each lattice site is host to a precise number of atoms, and there is no possible transport of atoms from one site to the next as shown in Fig 4.

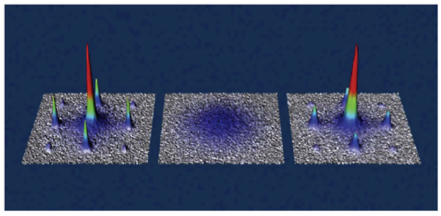


Figure 4: Momentum distribution of ultracold atoms in an optical lattice, illustrating the transition from a superfluid to a Mott insulator state and back. SOURCE: I.Bloch, Johannes Gutenberg University, Mainz, Germany.

Neutral atoms can be confined with electromagnetic fields to be nearly motionless forming well-defined crystals of atoms separated from each other. Unlike atomic ions, neutral atoms have no electric charge so they can only be held with laser beams or magnetic fields.

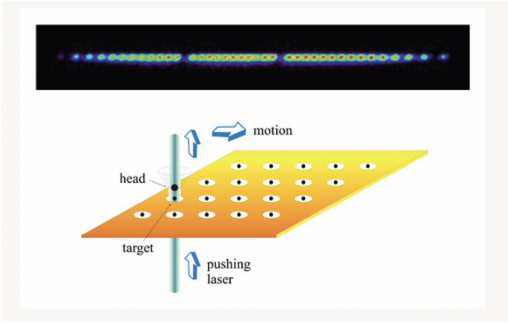


Figure 5: *Top*: Array of a few dozen trapped mercury ions. The ions fluoresce from applied laser radiation, and the apparent gaps are different isotopes that fluoresce at different wavelengths. SOURCE: J.Bergquist and D.wineland, National Institute of Standards and Technology. *Bottom*: Array of stationary trapped-ion quantum memories, with a single roving head ion interacting with any memory ion in order to move quantum information between memories. SOURCE: J.I.Cirac and P.Zoller, University of Innsbruck, Austria.

Pros of using optical lattice

- The separation between atoms in an optical lattice is thousand of times larger than the typical separation of atoms in a solid-state crystal and offers the possibility of doing controlled operations on qubits that are defined in terms of internal electronic states of the atoms. It can be seen from Fig 6, how the atoms trapped in a 2D optical lattice can be manipulated using the controlling laser fields.
- Optical Lattices present a fascinating way to avoid the decoherence that limits the realization of a practical quantum computer, through the creation of entangled states of atoms. Atoms produced in topologically protected quantum states- that is, quantum super positions of states whose relative phase is embodied only in many -particle, non local correlations-cannot have their states randomized by local interactions or interactions involving a single particle, which is generally how the environment causes decoherence. Such entangled states can therefore be more robust against decoherence [17].

Cons of using Optical Lattices

- Realisation of the current limitations on laser power.
- Considerations of parallelizability and optical access are seen to impose additional limits on the scalability of quantum computation with individually addressed gates.

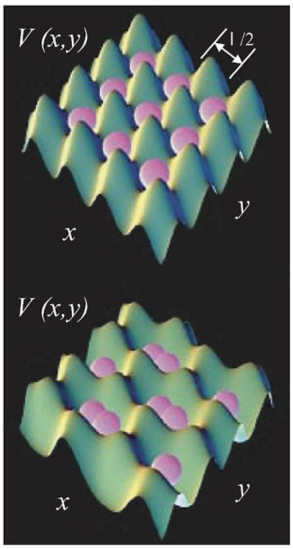


Figure 6: Controlling interactions of atomic qubits trapped in an optical lattice. *TOP*: Individual atoms (Purple) are confined in 2D potential wells formed by crisscrossed laser beams, spaced by one half of the optical wavelength. *Bottom*: By controlling the parameters of the external lasers, atoms can be made to approach and interact with the neighbours. SOURCE: National Institute of Standards and Technology.

G. Qubits Using Defects

A wave function on an isolated atom would provide an well-defined and well-understood quantum state for use as a qubit. Unfortunately, isolated atoms do not easily lend themselves to incorporation in a quantum devices therefore complex approaches like ion trap or optical lattices are required to constrain the atoms or ions. However, it turns out that the points defect in semiconductors can show the properties which are found similar to that of the isolated atoms as shown in Fig 7 .

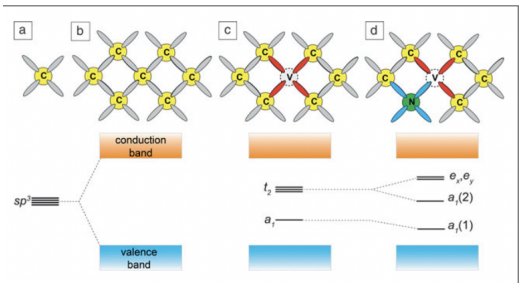


Figure 7: Schematic representation of the electronic structure of a point defect in a tetrahedral coordinated elemental semiconductor such as diamond. (a) The electronic states corresponding to the sp^3 orbitals on an isolated C atom. (b) The superposition of these orbitals that gives rise to the band structure of an infinite solid. The overlap of orbitals leads to bonding and anti-bonding states, which broaden into valence and conduction bands. If a carbon is removed, as shown in (c), a vacancy is created and the four orbitals on the surrounding atoms interact with each other in the tetrahedral environment ot give rise to states with a_1 and t_2 symmetry. Because the interaction between these orbitals is weaker than the C-C interaction that gives rise to the bands in the solid, the defect-related electronic states lie within the band-gap of the semiconductor. A symmetry lowering perturbation, such as incorporation of a nitrogen atom on one of the sites around the vacancy (d), further splits the t_2 states.

The electronic states associated with a vacancy tend to have energies that lie within the forbidden band-gap and their wave functions are constructed out of atomic orbitals on the neighboring atoms and are hence very localized on the scale of atomic dimensions. Nitrogen-vacancy (NV) centre in diamond is the prototype of point-defect qubit which consists of a nitrogen impurity next to a carbon vacancy. This centre can be initialized, manipulated and read out at room temperature using optical and microwave excitation, and electric and magnetic fields. Apart from this, the highly localized nature of the bound states of NV centre is critical in making a robust qubit and isolating from the sources of decoherence [18].

Some of the pros and cons of using point defects are given below:
Pros:
They are firmly embedded within the host material, and decades of investigation and characterization have provided us with many tools for controlling and manipulating such defects.
Cons:
When unintentionally present in semi-conductors, they can adversely affect the desired doping behaviour and lead to degraded electronic or optical properties.

3 Mott Insulators and Cold Atoms in Optical Lattices as Qubits for a Quantum Computer

Mott insulators are a class of materials that should conduct electricity under conventional band theories, but are in fact insulators when measured particularly in low temperatures. This effect is due to electron-electron interactions, which are not considered in conventional band theory. In general, Mott insulators occur when the repulsive Coulomb potential due to the electrons-electron interaction of the trapped atom is large enough to create an energy gap which restricts the flow of excited electrons.

Cold neutral atoms arranged in a large optical lattice have recently been proposed as a realization of qubit array. This approach was made possible by considerable advances in laser cooling and trapping of atoms. The neutral atoms in an optical lattice are coupled weakly to their surroundings and allow quantum operations to be performed in parallel on the whole lattice. They have a long coherence time and allow individual laser pulses to be used to initialize single qubits and to control their state and position.

An example of this is the application of the so-called Bose-Hubbard model to atoms in an optical lattice, as was done in 1998 by Jaksch *et al*, which was further well studied by Fisher *et al* . Fisher used this model to predict the behaviour of super fluid helium in porous media such as vycor. When a sufficiently deep optical lattice is applied to an harmonically trapped gas of bosonic atoms, a phase transition can be achieved from a super fluid phase to an insulating phase. The reason behind this phase transition is because when an optical lattice is loaded from Bose-Einstein condensate, the density of the atoms can be chosen such that there is on average exactly one particle at each lattice sites. When the lattice potential is relatively weak, the atoms can then tunnel between the lattice sites and the atoms can be still be seen in super fluid phase. However, when the lattice potential is very large, the two atoms on the same lattice site have a very large interaction energy as their relative distance is on average very small. This means that the tunneling between the lattice sites is strongly suppressed because an atom that tunnels to a neighbouring site has a high probability of encountering another atom. The reason behind this is it is quantum phase transition, which means it only occurs at zero temperature and is driven by competing terms in the free energy.[19]

4 SQUID

A SQUID (superconducting quantum interference device) is a very sensitive magnetometer used to measure extremely subtle magnetic fields, based on superconducting loops containing Josephson junctions. A squid

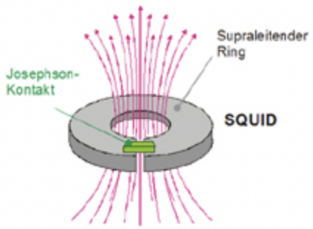


Figure 8: Schematic diagram of a superconducting ring. SOURCE: SQUID and Micro fabrication Technologies (Supracon), Germany

consists of one superconducting ring with two superconducting-insulating-superconducting (S-I-S) junctions. The operation principle of SQUID is based on Josephson effect and the flux quantization in a superconducting ring. The device consists of a superconducting loop interrupted by two Josephson junctions. When cooled below the critical temperature, the magnetic flux will be trapped in the loop. The super current (i_{supra}) causes

the magnetic flux to be a multiple of the fluxoid (ϕ_0). When ϕ_0 changes the superconductor adapts i_{supra} to compensate the total flux. Now the weak lines comes into play. I_{supra} cannot compensate large changes in the external magnetic field. When the critical current of the weak link is surpassed, superconductivity breaks down locally and a flux quantum can enter or leave the superconducting ring. This crossover happens instantly and is accompanied by energy dissipation between the weak link is in a resistive state. This dissipation can be accounted for very sensitively. This concept is also used for making very sensitive SQUID sensors.

4.1 SQUID as a quantum transistor:

SQUID are used as the basis for D-Wave systems 2000Q quantum computer[20] . As the name SQUID suggest interference in itself, which refers to the electrons that behave as waves inside a quantum waves. Interference of such quantum waves give rise to quantum effects. The reason that quantum effects such as electron waves are supported in such structure- allowing it to behave as qubit- is due to the properties of the material from which it is made. As seen in Fig. 9, the large loop in the diagram is made form a metal called niobium. When this metal is cooled down, it becomes what is known as a superconductor and starts to exhibit quantum mechanical effects. This superconducting qubit structure encodes 2 states as tiny magnetic fields, which

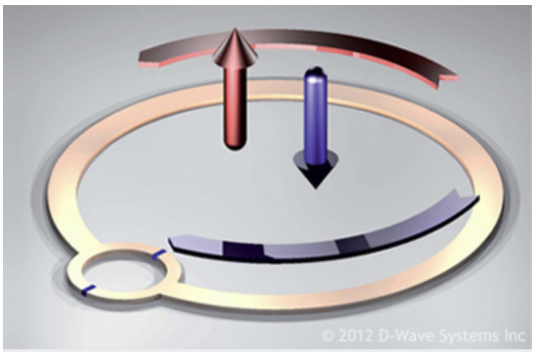


Figure 9: Schematic of a superconducting qubit, the basic building block of D-Wave quantum computer. The arrows indicate the magnetic spin states which encodes the bits of information as +1 and -1 values. Unlike regular bits of information, these states can be put into quantum mechanical superposition

either point up or down. We call these states +1 and -1, and they correspond to the two states that the qubit can 'choose' between. Using the quantum mechanics that is accessible with these structures, we can control this object so that we can put the qubit into a superposition of these two states. So by adjusting the knob on the quantum computer, it is possible to put all the qubits into a superposition state.

5 Quantum Error Correction Problem (Experimental Progress)

The idea that quantum error correction problem is possible is profound then the fact that we can do quantum computation with the perfect devices. It will even be possible to do quantum calculations with real devices because of the idea of quantum error correction. This idea is based on the fact that, if we try to measure any unknown quantum states, it will collapse. It will change randomly due to the back action resulting from the measurement. And if this unknown state develops error, it seems impossible but miraculously the error can be corrected.

Quantum information is stored not only in one physical qubit but in a logical qubit consisting of many physical qubits as seen in Fig 11. So the superposition of ground and excited state among different physical qubits in such a way that the 'Non-Locality' principle of putting the information on qubits is followed. No single physical qubits can know the state of the logical qubits because if that one qubit develops an error or is measured by environment ('decoherence'), we don't want the environment to learn the state of logical qubits and our system to collapse. To maintain coherence in the system, it is vital to hide all the information from the environment.

When the errors occurs in physical qubits, a Maxwell's Demon (Commercial FPGA with custom software) is required to correct those errors. Maxwell Demon is itself made of imperfect parts, which is very fast and accurate. It can make very clever measurements which tells what errors may have occurred and on which qubit so that the errors could be corrected.

Entropy is then pumped on to the cold bath to keep the logical states pure. Current industrial approach (IBM, Google, Intel

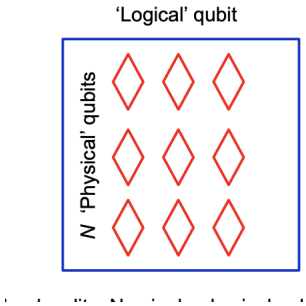


Figure 10: A logical qubit consisting of 9 physical qubits. SOURCE: Devoret et al., QuantumInstitute.yale.edu

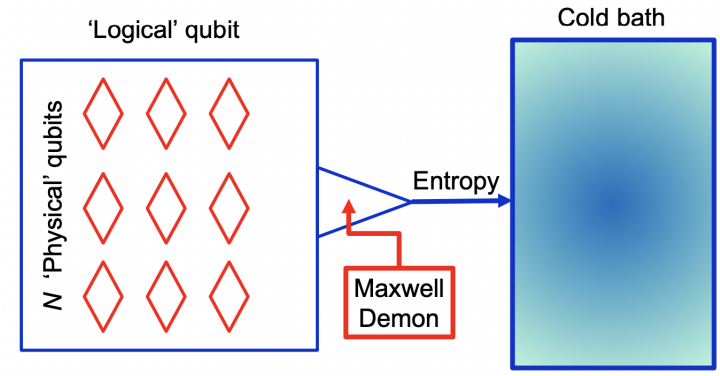


Figure 11: A logical qubit consisting of 9 physical qubits. N qubits have error N times faster and Maxwell demon must overcome this factor of N without introducing its own error. SOURCE: Devoret et al., QuantumInstitute.yale.edu

However, there is one big problem right off the cold bath. The N qubits have errors N times worse as each independent qubits might have errors of their own. Maxwell demon has to be very powerful and accurate to overcome this factor without adding its own error and get us back where the quantum information is on the single physical qubits. Because of this major problem, all the previous attempts to overcome the factor of N and reach the 'break even' point of QEC have failed. The reason is the because the Maxwell demon has to carry out the **error syndrome** and figure out all the different errors that could have occurred: Bit flip or Phase flip or their combinations and which of the N qubit suffered the error.

Because of the errors associated with N logical qubits and the challenge for Maxwell demon, Scientist come up with a different idea of not using material objects as qubits. Instead, they began the prospects of using microwave photon states stored in **high quality factor superconducting resonators.** The illustrated

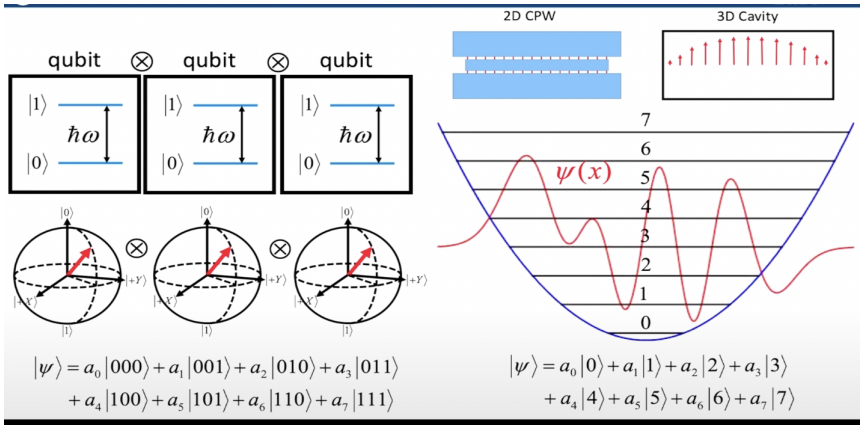


Figure 12: Comparison of two-level system and 3 qubits with 8 quantum states with the quantum amplitude stored in Physical qubits (In the left) and microwave photons (In the right). SOURCE: Devoret et al., QuantumInstitute.yale.edu

picture in Fig 12 represents 3 qubits with two level artificial atoms with 8 quantum states. Each of the eight quantum states can have quantum amplitude in the entangled correlated states of the logical qubits. So to

overcome the problems of errors in each different independent qubits and finding which qubit suffered the error as in the left part of Fig 12, microwave photons were inserted inside the cavity where there are exactly same number of quantum states with exactly the same 3 quantum amplitudes as stored in the 3 physical qubits shown in the right of Fig 12. The new system is continuous variable system $\psi(x)$, where we have discrete basis of photon number states where we store exactly the same information. [22].

5.1 Simplification and improvement of using Microwave Photons over Physical Qubits

1. The new system with microwave photons is one physical object; the cavity containing photons. This simplification of using one physical object with many states in its Hilbert space instead of many objects with only two in each of their states is an improvement.
2. The harmonic oscillator have only one kind of error. It can decay by loosing a photon. So it is just one possible mode with one possible error. And the loss of number of photon can be detected by measuring the photon number parity $P = (-1)^n$.

The errors detected can be corrected by using simplest Bosonic code example, or also known as continuous variable Quantum error correction code:

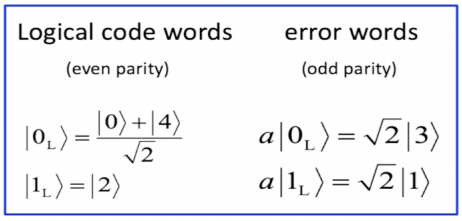


Figure 13: Simplest Bosonic code example: aka 'kitten code' uses only 5 photons states 0-4. SOURCE: Devoret et al., QuantumInstitute.yale.edu

In Fig 13, the Zero logical state is the coherence superposition of zero photons in the resonator plus the four photons in the resonator. Similarly, one logical state is two photons in the resonator.

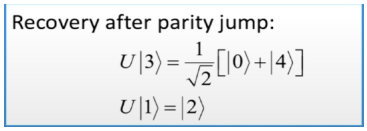


Figure 14: Simplest Bosonic code example: aka 'kitten code' uses only 5 photons states 0-4. SOURCE: Devoret et al., QuantumInstitute.yale.edu

After discovery of Shor's factoring algorithm, it was believed that the algorithm could not be implemented due to the inevitably intervention of errors. Moreover, quantum state are intrinsically delicate and has decoherence nature. Thus, the essence of Quantum Error Correction was realized. Prevalent classical fault tolerance technique was of no use due to "no-cloning" theorem and Heisenberg uncertainty principle.

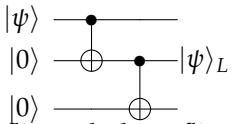
No-cloning theorem

$$U|0\rangle \nrightarrow |0\rangle|0\rangle$$
$$U(a|0\rangle + b|1\rangle) \nrightarrow (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)$$

The classical fault-tolerance techniques available are checkpointing, error-correcting codes, and massive redundancy. Checkpointing follows a cloning technique and not possible in quantum computation. Massive redundancy works for both classical and quantum computation but is not considered feasible. Error-correcting codes which are proved to be efficient than other techniques does not follow cloning technique, and hence works for quantum computation [7].
Error correcting protocols are based on adding redundant information. Initially, the qubits are encoded in three entangled qubits, known as logical qubit.

$$|0\rangle \rightarrow |0\rangle_L = |000\rangle$$
$$|1\rangle \rightarrow |1\rangle_L = |111\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow |\psi\rangle_L = a|000\rangle + b|111\rangle$$

This is encoding and not cloning. This is achieved using controlled NOT (C-NOT) gate.



After encoding we have to deal with bit flip and phase flip errors. Each is discussed here briefly.

A. Bit Flip

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

σ_x works against bit flip. This measurement is a projection onto one of four 2-d subspaces, generated by the vectors:

None bit flip: $\{|000\rangle, |111\rangle\}$ Bit 1 flip: $\{|100\rangle, |011\rangle\}$
Bit 2 flip: $\{|010\rangle, |101\rangle\}$ Bit 3 flip: $\{|001\rangle, |110\rangle\}$

Now, applying σ_x to incorrect bit corrects error.

B. Phase Flip

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$|0\rangle_L = |000\rangle \to |000\rangle = |0\rangle_L$$
$$|1\rangle_L = |111\rangle \to -|111\rangle = -|1\rangle_L$$

From above, it seems that a phase flip on any qubit gives a phase flip on the encoded qubit, thus phase flips are three times as likely though we overcome the problem of bit flip.

The unitary transformation called Hadamard gate takes phase flips to bit flips and vice versa.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$H\sigma_x H^\dagger = \sigma_z$$
$$H|0\rangle_L = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$$
$$H|1\rangle_L = \frac{1}{2}(|100\rangle + |010\rangle + |001\rangle + |111\rangle)$$

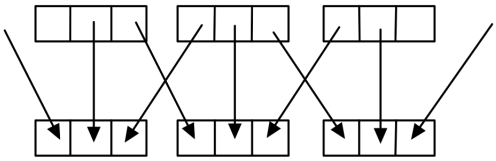
After applying H, it is evident from above that bit flips are three times likely since a bit flip on any qubit exchanges 0 and 1 and takes a logical 0 to logical 1.
Combining these 3 qubit codes which corrects bit flip and phase flip, it gives 9-qubit code. Encoding the qubit with one 3-qubit code first, and then encoding the result with other 3-qubit code protects against both phase and bit flip errors, called *concatenating* the codes. This way, first quantum error correcting code [8] was discovered, which corrects any error in one of the nine qubits.

$$|0\rangle_L = \frac{1}{2}(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle)$$
$$|1\rangle_L = \frac{1}{2}(|111000000\rangle + |000111000\rangle + |000000111\rangle + |111111111\rangle)$$

Now to address the problem imposed by **Heisenberg uncertainty principle**, i.e. if error is measured, the state of the system is disturbed, the codes are constructed beforehand where the error can be measured (assuming it falls into some set of likely errors) without measuring the encoded quantum state. We then can correct the error without disturbing the quantum state. This, however, requires us to find codes where the likely errors are orthogonal to the encoded state.

6 Quantum Cellular Automata as Model of Quantum Computation

Quantum Cellular Automata has been proposed as a computational abstract model for quantum computer. The highlight of Quantum Cellular Automata is that with its homogeneity of local interactions and uniformity of rules applied parallel across the lattice of qubits, the individual qubits in the lattice need not be separately addressed. The qubits form a network, and the state of the qubit is determined by its current state and that of its neighbours. The evolution acts the same anywhere and is independent of time. In such regard, QCAs can effectively model a Quantum Turing Machine.
A kind of a model proposed is *one dimensional quantum cellular automata*, or the more restricted class of 1d-QCA called *one dimensional partitioned quantum cellular automata* (1d-PQCA). A 1d- PQCA is a 1d- QCA in which each cell is partitioned into three sub-cells (left, middle, and right), and where the next state of any given cell depend only on the contents of the right sub-cell of its left neighbour, the middle sub-cell of itself, and the left sub-cell of its right neighbour. [9]



Other such a model proposed is using coupled quantum dot cells. A QCA consists of an array of quantum-dot cells connected locally by the interactions of the electrons contained in each cell. The quantum state of each cell is used to encode binary information, and the Coulomb interaction connects the state of one cell to the sate of its neighbours. [10]
We would like to go in detail through used for quantum computation and simulation of quantum systems.

6.1 Watrous Model

To understand 1d-PQCA, it is necessary to understand about 1d- QCA, which is represented as a quadruple (Q, δ, k, A), where Q is a finite set of *states* (including non-active states denoted by ϵ), δ is a *local transition function*, k is an integer denoting the acceptance cell, and $A \subseteq Q$ is a set of *accepting states*. M is a two-way infinite sequence of cells, indexed with integers $\mathbb{Z}$.
The local transition function δ is a map

$$\delta : Q^4 \to \mathbb{C}$$

with

$$\delta(\epsilon, \epsilon, \epsilon, q) = \begin{cases} 1 & q = \epsilon \\ 0 & q \neq \epsilon \end{cases}$$

which describes the evolution of M.
A configuration of a 1d-QCA M is a map

$$a : \mathbb{Z} \to Q$$

where, for each integer n, $a(n)$ denotes the state of the cell indexed by n. Each cell evolves simultaneously in this way, so that globally if M in some configuration a, at time t, then M' at time $t+1$ is in configuration b with associated amplitude

$$\prod_{n \in \mathbb{Z}} \delta(a(n-1), a(n), a(n+1), b(n))$$

Thus, M can evolve in multiple ways. The evolution of multiple paths with different associated amplitudes occurs simultaneously, and the probability to observe a given configuration is its square of the amplitude associated with the particular configuration. It is necessary for the probabilities to sum 1, which imposes an additional constraint in δ. The automata with constrained local transition function is called *well-formed*[9]. Bernstein and Vazirani has shown that such *well-formed* is *Turing complete* [11]. It is shown in [9] to construct a restricted local transition function in 1d-PQCA, which is *well-formed.*
A quantum Turing machine M is a quintuple (K, Σ, μ, k, A) where K is a finite set of states, Σ is a finite *tape alphabet* (similar to Turing machine, including a distinguished *blank* symbol), μ is a *local transition function*, k is an integer indexing distinguished *acceptance tape square*. M has similar read-write tape head as in Turing machine. Showing $M_{ca} \in$ 1d-PQCA $\Leftrightarrow$ $M_{tm} \in$ QTM [9], we can simulate a Turing machine with Quantum Cellular Automata.

6.2 Schumacher-Werner QCA and General Margolus Partitioned QCA

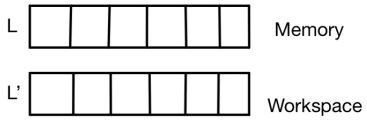
Schumacher-Wernes takes an approach using Heisenberg picture. The evolution of the algebra of observables on the lattice are only considered rather than the state of the cell lattice itself. Let $\mathcal{A}(S)$ denotes the set of all observables on finite subsets $S \subseteq L$ of the lattice and extended on the entire lattice by taking tensor product with the identity operator. QCA is defined in lattice L, the neighbourhood scheme $\mathcal{N}$, the single-cell observable algebra $\mathcal{A}$, and the global transition operator defined as a homomorphism $T : \mathcal{A}(L) \to \mathcal{A}(L)$. The local transition operator is simply a homomorphism $T_0 : \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$, from the observable algebra of a single-cell to the observable algebra of the neighbourhood of that cell, related to global transition as

$$T(\mathcal{A}(S)) = \prod_{x \in S} T_x(\mathcal{A}_x)$$

Using Margolus partitioning scheme, Schumacher and Werner extended the model to include the reversibility ability [12].

6.3 Shift-Right QCA

After Toffoli [13] showed that any reversible cellular automata can be modeled as a Turing machine, it was then required to come up with an idea of building reversible cellular automata. Watrous QCA Model and Schumacher-Werner QCA Model were not unitary and local [14]. Thus, to highlight the importance of use of local unitary operators, a QCA model called *Shift-right QCA* was proposed [15]. In 1-dimensional *Shift-right* QCA, a cell denoted by x would store the state $|\psi_{x-k}\rangle$ after k updates. The This is obviously reversible, whose inverse being *Shift-left* QCA. In fact, such QCA cannot be implemented by any local unitary process [15]. Thus, to make use of local unitary operations, a *Shift-right* QCA is retooled to use a second lattice L' of same dimension of original lattice L. The output of the configuration is written to L', after local transition function is applied to each cell. After this, copy the information from L' to L using appropriate single-cell update operation to each cell.



If we want this model to be reversible, then local transition function and the cell update function have to be reversible. However, the initial state of the memory lattice cannot be reset in a reversible model. To solve this, each configuration $C \in L$ is matched with its dual memory configuration $C' \in L'$. Such a construction is realized as $\mathcal{A} = (L, \Sigma, \mathcal{N}, f)$ with global transition function $F : \Sigma^L \to \Sigma^L$, and $\mathcal{A}'$ with global transition function $F' : \Sigma^L \times \Sigma^{L'} \to \Sigma^L \times \Sigma^{L'}$ if there exits a bijection $D : \Sigma^L \to \Sigma^{L'}$ such that $F'(C, D(C)) = (F(C), D(F(C))$, with $D = F^{-1}$. Then, it is easy to show that global transition function F' will clear the memory lattice by computing the reverse configuration $F'(C)$ and subtracting it from the memory lattice then computing the next configuration F(C). That is

$$C \xrightarrow{F^{-1}} F^{-1}(C) \xrightarrow{output} \square \to \square \to C$$
$$\square \to \square \to F^{-1}(C) \xrightarrow{F} C \xrightarrow{update} \square$$

It is shown that such QCA can effectively simulate quantum circuit in [15]. Thus, it fulfills our all desired properties of QCA listed below.

- Reversibility
- Local Unitary Operations
- Capable of simulating a Quantum Circuit
- Able to model space- and time-homogenous phenomena

Quantum annealing (QA) Quantum annealing is a meta-procedure for finding a global minimum of a given objective function over a given set of candidate solutions by a process using quantum fluctuations. It is used mainly for problems where the search space is discrete with many local minima. In other words, Quantum

annealing simply uses quantum physics to find low-energy states of a problem and therefore the optimal or near-optimal combination of elements. This procedure was first proposed in 1988 by B. Apolloni, N. Cesa Bianchi and D. De Falco.[1]It was formulated in its present form by T. Kadowaki and H. Nishimori in 'Quantum annealing in the transverse Ising model.[32]

7 Quantum Annealing in D-Wave Systems

Quantum bits, also known as qubits, are the lowest energy states of the superconducting loops that make up the D-wave quantum processing unit. A qubit can be in state of 0 or 1 and these states have a circulating current and a corresponding magnetic field or the superposition of the 0 state and 1 state a the same time. At the end of the quantum annealing process, each qubit collapses from a superposition state into either 0 or 1. The physics behind this process can be seen in *Fig*16. The diagram changes over time as shown in (a), (b) and

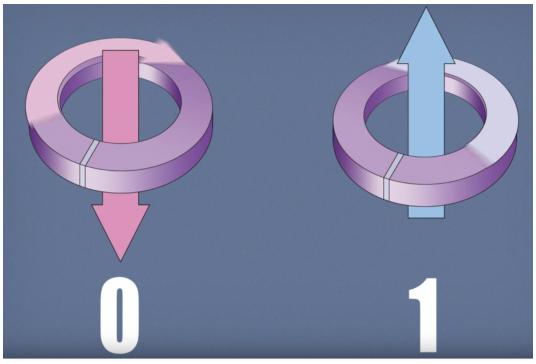


Figure 15: A qubit's state is implemented as a circulating current, shown clockwise for 0 and counter clockwise for 1, with a corresponding magnetic field. SOURCE: D-Wave Systems Inc

(c). To begin, there is just on valley in figure (a), with a single minimum. The quantum annealing process runs, the barrier is raised, and this turns the energy diagram into what is known as double-well potential as seen in (b). Here, the low point of the left valley corresponds to state 0 and the low point of right valley corresponds to state 1. The qubits ends up in one of these valleys at the end of the anneal. The probability of

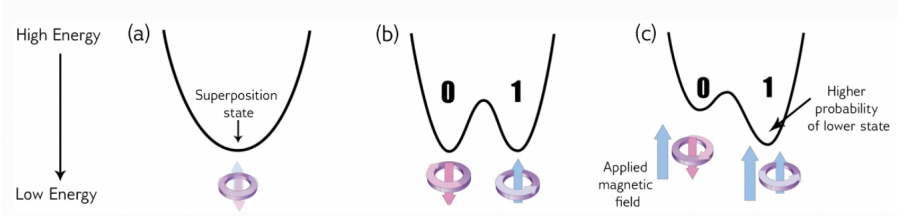


Figure 16: Energy diagram changes over time as the quantum annealing process runs and a bias is applied. SOURCE: D-Wave Systems Inc

the qubit ending in the 0 or 1 state is 50 percent each. However, by applying an external magnetic field the probability of it falling into 1 or 0 state can be manipulated as shown in *Fig*16 (c). The external field tilts the double-well potential, increasing the probability of the qubit ending up in the lower well. The programmable quantity that controls the external magnetic field is called bias, and the qubit minimizes its energy in the presence of the bias.
Bias term alone is not very useful. The real power of the qubits is obtained when the qubits are linked together so that they can influence each other. This can be done with a device called a coupler. A coupler can make two qubits tend to end up in the same state- both 0 or both 1- or it can make them tend to be in opposite states. Similar to that of bias qubit, the coupled qubits can also be programmed by setting a coupling strength. Coupler uses the phenomena of entanglement. The entangled two qubits can be thought as a single object with four possible states which can be illustrated as shown in *Fig*17 Fig 17 illustrates the idea of showing potential with four states, each corresponding to a different combinations of two qubits: (0, 0), (0, 1), (1, 1), and (1, 0) where their relative energy depends on the biases of qubits and coupling between them.[25]

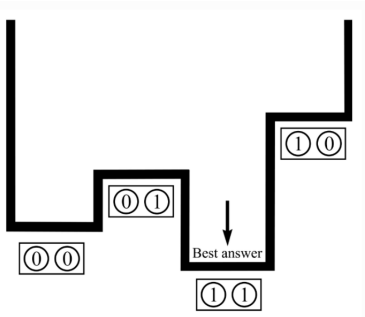


Figure 17: Energy diagram showing the best answers.

When formulating a problem, users choose values for the biases and couplers. The biases and couplings define an energy landscape, and the D-Wave quantum computer finds the minimum energy of that landscape: this is quantum annealing. As the qubits are added, systems get increasingly complex. Each additional qubit doubles the number of states over which you can define the energy landscape: the number of states goes up exponentially with the number of qubits.

8 Simulated Annealing and Quantum Simulated Annealing

The idea of simulated annealing (SA) was first proposed by Kirkpatrick *et al* as a general method to solve optimization problems[30] . The idea of simulated annealing is to use thermal fluctuations to allow the system to escape from local minima of the cost function so that the system reaches the global minimum under an appropriate annealing schedule. If the temperature is decreased too quickly, the system may become trapped in a local minimum. Too slow annealing, on the other hand, is practically useless although such a process would certainly bring the system to the global minimum. Geman and Geman proved a theorem on the annealing schedule for a generic problem of combinatorical optimization[31] . They showed that any system reaches the global minimum of the cost function asymptotically if the temperature is decreased as $T = \frac{c}{log(t)}$ or slower, where c is a constant determined by the system size and other structures of the cost function. This bound on the annealing schedule may be optimal one under generic conditions, however, in practical applications is many system the faster decrease in the temperature often gives satisfactory results. SA is a possible generic strategy for solving a Combinatorical optimization problems (COPs)[30] . The idea of SA is to imitate the process undergone by a metal that is heated to a high temperature and then cooled slowly enough for thermal excitation to prevent it from getting stuck in local minima, so that it ends up is one of its lower-energy states. In SA, the objective function plays the role of energy so the lowest state is the optimum. The process can be simulated using different techniques like discrete Markov chain Monte-Carlo (MCMC), quantum tunneling process for state transitions and so on.

In Quantum Annealing (QA) approach, a time-dependent quantum transverse field is added to the classical energy function leading to an interpolating Hamiltonian that may take advantage of correlated fluctuations mediated by tunneling. Starting with a high transverse field, the model can be initialized in its ground state: i.e all spins are aligned in the direction of the field. The adiabatic theorem then ensures that by slowly reducing the transverse field, the system remains in the ground state of the interpolating Hamiltonian. At the end of the process, the transverse field vanishes and the system ends up in the sought ground state of the classical energy function. The original optimization problem would be solved if the overall place could take place in a time bounded by some low-degree polynomial in the size of the problem. Unfortunately the adiabatic process can become extremely slow. The adiabatic theorem requires the rate of change of the Hamiltonian to be smaller that the square gap between the ground state and first excited state. For small gaps the process becomes inefficient.

Quantum annealers are physical quantum devices designed to solve optimization problems by finding low-energy configurations of an appropriate energy function by exploiting cooperative tunneling effects to escape local minima. Quantum annealing can be compared to simulated annealing, whose 'temperature' parameter plays similar role to QA's tunneling field strength. In simulated annealing, the temperature determines the probability of moving to a state of higher 'energy' from a single current state. Where, in quantum annealing, the strength of transverse field determines the quantum-mechanical probability to change the amplitudes of all states in parallel as shown in Fig: 19

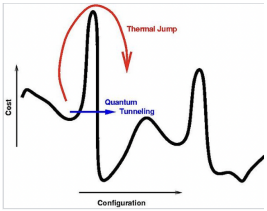


Figure 18: rugged cost/energy lasdscape showing that the thermal jump has to be over the barrier (in red) but the quantum tunneling may be through the barrier (in blue). Thus quantum tunneling may be more efficient means of traversing the rugged landscape when the barriers are tall but thin [33].

8.1 General explanation on Markov chain Monte Carlo methods

MCMC methods crates samples from a continuous random variable, with probability density proportional to known function. These samples can be used to evaluate an integral over that variable as its expected value or variance.

Practically, an ensemble of chains is generally developed, starting from a set of points arbitrarily chosen and sufficiently distant from each other. These chains are stochastic process of 'Walkers', which in a sense move around randomly according to an algorithm that look places with a reasonably high contribution to the integral to move into next, assigning them higher desired probabilities.

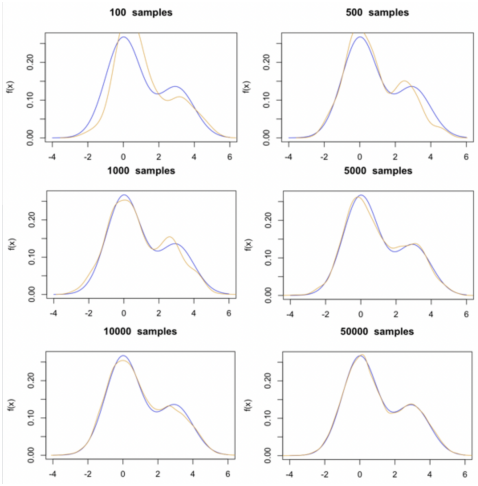


Figure 19: Convergence of the Markov Chain Monte Carlo method to approximate the blue distribution with the orange distribution

Although MCMC methods were created to address multi-dimensional problems, when the number of dimensions rises they tend to suffer the curse of dimensionality: regions of higher probability tend to stretch and get lost in an increasing volume space that contributes to the integral. One way to address this problem could be shortening the steps of the walker, so that it doesn't continuously try to exit the highest probability region and the walker stays mostly around our desired area. However, in this way the process would be highly auto-correlated and expensive as many steps would be required for an accurate result.[30]

8.2 Companies that are closest to bringing quantum annealing to the market

- In 2011, the first commercial quantum annealing machine, operating on a 128 qubit was developed by D-Wave which cost about US 10,000,000 dollars. D-Wave (founded in 1999) is the first to introduce a quantum annealing approach in order to implement in a quantum computer. In February 2019, D-Wave announced 'Pegasus' which is a quantum processor chip that consist of 5,000 low-noise qubits.
- The other player for quantum annealing is Japanese company NEC corporation. In December 12, 2018 the company introduced a research program for the development of quantum annealing machine

8.3 The Hamiltonian of D-Wave systems

For the D-Wave system, the Hamiltonian may be represented as:

$$H = -\frac{A(s)}{2}\left(\sum_i {\sigma_x}^i\right) + \frac{B(s)}{2}\left(\sum_i h_i {\sigma_z}^i + \sum_{i>j} J_{i,j}\sigma_z^i\sigma_z^j\right)$$

where $\sigma_{x,z}^i$ are pauli matrices operating on qubit q_i and h_i and $J_{i,j}$ are the qubit biases and coupling strengths. And the Hamiltonian is the sum of two terms:

- First Hamiltonian: It comprises the lowest energy state when all qubits are in a superposition state of 0 and 1. This term is also called the tunneling Hamiltonian.
- Second Hamiltonian: The second term is called the problem Hamiltonian, and it includes the qubit biases and the couplings between qubits.

In quantum annealing, the system begins in the lowest energy eigenstate of the initial Hamiltonian. As it anneals, it introduces the problem Hamiltonian, which contains the biases and couplers, and it reduces the influence of the initial Hamiltonian. At the end of the anneal, it is an eigenstate of the problem Hamiltonian. So, theoretically it has stayed in the minimum energy state throughout the annealing process so that at the end it is in the minimum energy state of the problem Hamiltonian which is our required answer. At the end of the anneal, each qubit is a classical object.

9 Quantum Cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. It is one of the emerging topics in the field of quantum-computing industry. One of the best known example of quantum cryptography is quantum key distribution, which offers an information-theoretically secure solution to the key exchange problem. Some of the cryptographic tasks which are proven to be impossible using non-quantum communications are possible using quantum cryptography. For example, it is impossible to duplicate the data encoded in a quantum state. If there are interruptions, the quantum state of the data will be changed due to wave function collapse (no-cloning) theorem.

9.1 Quantum cryptography in theory

The theoretical basis of quantum cryptography takes in account of Heisenberg Uncertainty principle and principle of photon polarization. According to the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Which implies that the polarization of the particle is only known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principles describes how light photons can be oriented or polarized in specific directions. Moreover a photon filter with the correct polarization principle only detect a polarized photon or else the photon will be destroyed. It is the 'one-way-ness' of photons along with the Heisenberg Uncertainty principle that makes quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

9.2 Implementation in practice

In theory, quantum cryptography seems to be unconditionally' successful turning point in the information security sector. However, no cryptographic method can ever absolute secure.[27] . In practice quantum cryptography is only conditionally secure, dependent on a key set of assumptions.

9.2.1 Heisenberg Uncertainty principle and Single-photon source assumption

The theoretical basis for quantum key distribution assumes a single-photon source. However, single-photon sources are difficult to construct. In-fact, most real-world quantum cryptography systems use faint laser sources as a medium for information transfer.[28]. This multi-photon sources due to faint laser sources open a pathway for eavesdropper attacks, particularly a photon splitting attack. Eve can split the multi-photon source and retain one copy for herself. The other photon can be transmitted to Bob without any trace that Eve captured a copy of the data. The criteria needed to achieve a perfectly single-photon sources are very demanding due to difficulties in device growth and fabrication, and therefore such a device has not yet

been accomplished. The standards held by quantum information applications state that there are three main characteristics of an ideal source should emit single photons is emitted per excitation pulse with a vanishing probability of multi photon emission. Second, once emitted, each photon should be collected with high efficiency in the desired quantum channel, ideally with near-unitary efficiency. Third, the single photons emitted should be indistinguishable, meaning that each photon is identically in every way, for example, having same polarization, spatial mode and temporal profile to allow near-perfect quantum interference. However, in 2016, scientists developed a near perfect single photon source as shown in Fig 20 and estimates that one could be developed in the near future.[28]

9.2.2 Theory of realising a single-photon source

Exciting of an electron in a semiconductor from the valence band to the conduction band creates an excited state, a so called excition. The spontaneous radioactive decay of this exciton results in the emission of a photon. Since a quantum dot has discrete energy levels, it can be achieved that there is never more than one excition in the quantum dot simultaneously. Therefore, the quantum dot is an emitter of single photons.

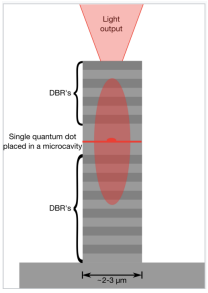


Figure 20: Schematic structure of an optical microcavity with a single quantum dot placed between two layers of distributed Braggs reflectors. The asymmetry in the structure is crucial for high-efficiency, polarized single-photon emission.

The is, however, a challenge to make sure that the emission from quantum dot is collected efficiently. In order to do that, the quantum dot is placed in an optical cavity as shown in Fig: 20. The cavity consists of two distributed Braggs reflectors (DBRs) in a micro-pillar which enhances the spontaneous emission in a well-defined optical mode, facilitating efficient guiding of the emission into an optical fiber[29] . In addition to that, the significantly reduced excitation lifetime also reduces the significance of line-width broadening due to noise. Also to ensure the probability of simultaneous emission of two photons, it is made sure that there can only be one exciton in the cavity at one time which is allowed by the discrete energy levels of the quantum dot. However, there is always a small probability of existing two excitons confined in a small volume which are called as biexcitons. They interact with each other and thus slightly change their energy. They can be filtered out by letting the outgoing beam pass an optical filter. In order to have the highest probability of creating an exciton, the optical pumping laser is turned on resonance[29] . This resembles a π-pulse on the Block sphere. However, the pump laser and the emitted photons will have the same frequency. A polarizer is therefore required to separate them.

9.3 Application

One of the most important applications of quantum cryptography is quantum key distributor which is discussed below:

9.3.1 Quantum key distribution (QKD)

QKD is a application of quantum cryptography which is a process of using quantum communication to establish a shared key between two parties (for instance: Alice and Bob) without letting a third party (Eve) know anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. Alice begins by sending a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarization that corresponding to vertical, horizontal or diagonal in opposing directions. Bob will randomly choose a filter and use a photon receiver to count and measure the polarization filter on which the measurements are vis-à-vis the polarisation that Alice selected. The photons that were incorrectly measured will be discarded, while the correctly measured photons are translated into bits based on their polarization. The photons are used to form the basis of one-time pad for sending encrypted information. It is important to point out that neither Alice nor Bob are able to determine what the key will be in advance because the

key is the product of both their random choices. Thus, quantum cryptography enables the distribution of a one-time key exchanged successfully.
Now, Eave will have to randomly select a rectilinear or diagonal filter to measure each of Alice's photons. Hence, Eve will have an equal chance of selecting the right and wrong filter, and will not be able to confirm with Alice the type of filter used. Even if Eve successfully eavesdrop while Bob confirms with Alice the protons he received, the information will be little use to Eve unless she knows the correct polarization of each particular photon. Thus, Eve will not correctly interpret the photons that form the final key, and she will not be able to render a meaningful output. In total, there are three significant advantages of this system:

- According to the Heisenberg Uncertainty principle, information on photons will not be duplicated as photons will be destroyed as they are measured or tampered with. And as the photons are indivisible, once they hit the detector they no longer exist.
- Bob must calculate beforehand the amount of photons needed to form the encryption key so that the length of one-time pad will correspond to the length of the message. Bob will receive a fixed number of transmitted photons from Alice, if there is a derivation from the predetermined fixed number, Bob can be certain that the traffic or something is wrong on the system. This is the result of Eve detecting a photon which explains the missing photon number encountered by Bob.
- If Eve tries to create and pass photons on to Bob, she will have to randomly choose its orientation and on average be incorrect about 50 percent of the time, which is enough of an error rate to reveal her presence.

10 Quantum Systems as Local Unitary Quantum Cellular Automata

10.1 Quantum Spin Chains

A Quantum Spin Chain Model is realized to construct a type of Local Unitary Quantum Cellular Automata, which fulfills all those desired properties of QCA. It consists of 1-dimensional lattice of identical quantum systems, say spin-$\frac{1}{2}$ with ϵ as absence of a particle in open chain. The interaction between n and $n+1$ cells is described by a coupling Hamiltonian $H^{(n,n+1)}$, and the Hamiltonian for the entire chain of length N is

$$H = \sum_{n=1}^{N-1} H^{(n,n+1)}$$

Say the evolution of the system is discrete in time step Δt, with unitary time evolution

$$U_L = e^{-iH\Delta t/\hbar} = e^{-iH\Delta t}; \hbar = 1$$

A. Ising Spin Chain
The Ising interaction is given by

$$H^{(n,n+1)} = J\sigma_z^{(n)}\sigma_z^{(n+1)}$$

on neighbouring spins, where J is a coupling strength constant. Thus, the Hamiltonian for the entire chain will be

$$H = \sum_{n\in L} H^{(n,n+1)} = \sum_{n\in L} J\sigma_z^{(n)}\sigma_z^{(n+1)}$$

In Ising Spin chain system, the local interaction between spins is translate commutative, i.e. $[H^{(n,n+1)}, H^{(m,m+1)}] = 0$ for all $n, m \in L$. Thus,

$$U_L = e^{-iH\Delta t} = \exp\left(-i\sum_{n\in L} H^{(n,n+1)}\Delta t\right) = \prod_{n\in L}\exp(-iH^{(n,n+1)}\Delta t)$$

Let $U_n = \exp(-iH^{(n,n+1)}\Delta t$. Since $H^{(n,n+1)}$ is translate commutative, U_n is also translate commutative, which now can simulate the evolution of an Ising Spin Chain

B. Heisenberg Spin Chain
In Heisenberg Spin Chain, the local interactive Hamiltonian is not translate commutative.

$$H^{(n,n+1)} = J(\sigma_x^{(n)}\sigma_x^{(n+1)} + \sigma_y^{(n)}\sigma_y^{(n+1)} + \sigma_z^{(n)}\sigma_z^{(n+1)} - \mathbb{1}\otimes\mathbb{1})$$

Thus, only the approximation of evolution of Hamiltonian can be made using *Suzuki-Trotter Decomposition*, which for Hermitian operators A and B and $\delta > 0$ is

$$\left\| e^{\delta(A+B)} - e^{\delta A \delta B} \right\| = O(\delta^2) \left\| [B, A] \right\|$$

Let,

$$H_a = \sum_{n \in L} H^{(2n,2n+1)}$$

and

$$H_b = \sum_{n \in L} H^{(2n-1,2n)}$$

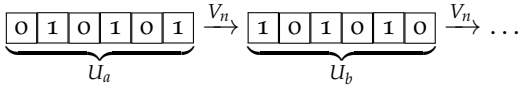
and set $A = -iH_a\Delta t, B = -iH_b\Delta t$ and $\delta = \frac{1}{k}; k \in \mathbb{R}$. Thus,

$$e^{-i(H_a+H_b)\Delta t} = \left(e^{-iH_a(\Delta t/k)} e^{-iH_b(\Delta t/k)} \right)^k + O(\frac{1}{k}) \left\| [H_a, H_b \right\| \Delta t^2$$

Since H_a and H_b are constructed on disjoint neighbourhood, they are pairwise commuting, and

$$U_a = e^{-iH_a(/k)} = \exp\left(-\frac{i\Delta t}{k} \sum_{n \in L} H^{(2n,2n+1)} \right) = \prod_{n \in L} U_{2n}$$
$$U_b = e^{-iH_b(\Delta t/k)} = \exp\left(-\frac{i\Delta t}{k} \sum_{n \in L} H^{(2n-1,2n)} \right) = \prod_{n \in L} U_{2n-1}$$

where $U_n = \exp(-iH^{(n,n+1)}(\Delta t/k))$, which is not translate commutative. Set $\mathcal{N} = \{0, 1\}$ and control register $\Sigma_2 = \{0, 1\}$, initialized to $|0\rangle$ for even-indexed cells $2n$, and $|1\rangle$ for odd-indexed cells $2n-1$, and applying U_n, which acts only if the configuration is $|01\rangle$, and is now translate commutative. The single-cell update function V_n flips the control bit, thus the global transition function alternates between applying U_a and U_b, as desired, which now can simulate the evolution of Heisenberg Spin Chain [15].



10.2 Entanglement Dynamics in QCA

Since entanglement can be shared in different ways by different subsets (parties) of the spins in the lattice, there does not exist a single function invariant under local unitarians U_j that describes multipartite entanglement. Let's define a function on pure staes of n qubits that quantifies the amount of multi-spin entanglement as

$$R(|\psi\rangle) = 2\left(1 - \frac{1}{n}\sum_{j=0}^{n-1} \mathrm{Tr}[\rho_j^2]\right); 0 \leq R(|\psi\rangle) \leq 1; R(|\psi\rangle) = \begin{cases} 0 & \text{product states} \\ 1 & \text{some entangled states} \end{cases}$$

This, however, cannot distinguish subglobal entanglement. Say, for $n = 4$, the product state of two maximally entangled Bell states and the four-spin GHZ state both have R values 1. This is often tackled by examining temporal variation of Schmidt numbers of the state $|\psi\rangle$ over the set of all $2^{(n-1)}$ bipartite divisions of the n lattice qubits.

Some examples:

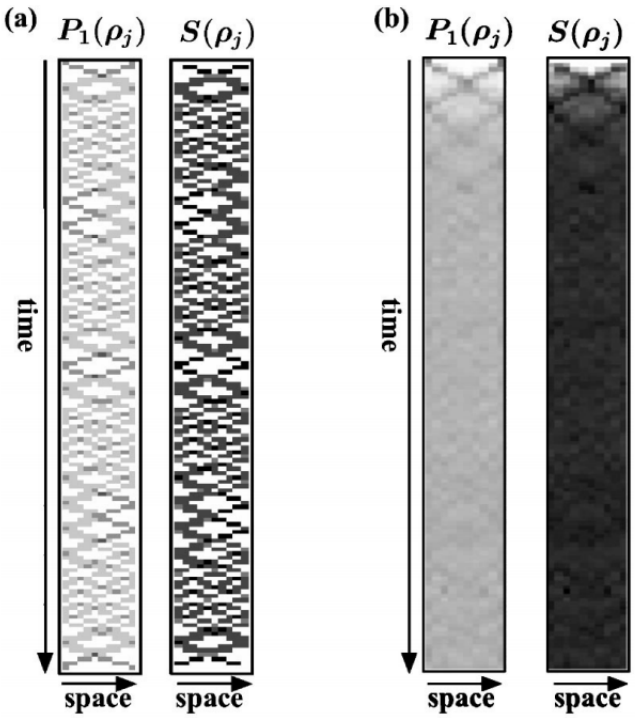


Figure 21: Entanglement dynamics visualized by the space-time histories of the evolution of a chain of ten spins by two BQCA rules. The boundaries are fixed at $|0\rangle$ and the initial state is the same for both rules with all qubits initialized to $|0\rangle$ except for the qubits at sites 0 and $n-1$ each in the superposition state $1/\sqrt{2}(|0\rangle + |1\rangle)$. (a) Rule $M(1, e^{-i(\pi/2)\sigma_x}, e^{-i(\pi/2)\sigma_x}, e^{-i(\pi/2)\sigma_x})$. (b) Rule $M(1, e^{-i(\pi/4)\sigma_x}, e^{-i(\pi/4)\sigma_x}, e^{-i(\pi/4)\sigma_x}$. [16]

Appendix

A Universities on Quantum Computing

During the internship, we came across various resources and knew about different research projects being organized at different universities across the globe. This gives us inspiration and information on state of the art in quantum computing. Few of them are listed here.

A. Ludwig-Maximilians-Universität München and Technical University of Munich
The two universities work together as a part of Munich Center for Quantum Science and Technology. The quantum computing group aims to pursue new experimental techniques, while collaborations with Quantum Information Theory, Quantum Simulation, and Quantum Matter to develop ideas of topological matter and quantum control to address decoherence. The goals are listed as

- Understand, control, and shape entanglement in quantum many-body systems
- Overcome the apparent fragility of quantum information
- Store quantum information over sufficiently long time scales
- Realize high fidelity quantum operations
- Implement quantum error correction without a considerable experimental overhead

The group is funded by Deutsche Forschungsmeinschaft under Germany's Excellence Strategy in partnership with Max Planck Institute of Quantum Optics, Walther-Meissner-Institute and Deutsches Museum.

B. University of Waterloo
The Institute for Quantum Computing, as an affiliate scientific research institute of University of Waterloo, is focused on diverse topics. Few of them includes

- Using spin property to encode quantum information

- Using ultracold matter to study complexities of many-body quantum systems and macroscopic quantum phenomena
- quantum communication and quantum encryption, extending the distance for transferring quantum information
- Quantum Information with trapped ions to create a flexible quantum system with control at the level of individual particle

The institute is in partnership with IBM.

C. California Institute of Technology
CalTech's Insititute for Quantum Information and Matter is a National Science Foundation Physics Frontiers Center. The distinguished research works are

- High-fidelity entanglement and detection of alkaline-earth Rydberg atoms
- Converting a superconducting qubit to an optical photon
- Study of quantum effects in Ising spin systems

The institute is funded by NSF Physics Frontiers and CERN.

D. RWTH Aachen University
RWTH Aachen University, under Jülich Aachen Research Alliance, focuses its research on

- Study of solid-state qubits based on superconducting and spin
- Long range on chip qubit coupling
- Scanning SQUID microscopy
- Topological quantum computing and error correction in system of trapped ions

The institute is also in collaboration with Matter and Light for Quantum Information as part of German Research Foundation.

Other several universities like ETH Zürich, University of Barcelona, University of Wisconsin-Madison, in partnership with different institutes are also in research about quantum computing.

References

[1] DiVincenzo, D. P. & IBM. The Physical Implementation of Quantum Computation. arXiv:quant-ph/0002077 (2000)

[2] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects.* Washington, DC: The National Academies Press.

[3] He-Liang Huang, Dachao Wu, Daojin Fan, and Xiaobo Zhu. Superconducting Quantum Computing: A Review. November 3, 2020.

[4] Colin D. Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M. Sage. Trapped-Ion Quantum Computing: Progress and Challenges. *Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, MA, 02420*. April 9, 2019

[5] Franson J.D., Jacobs B.C., Pittman T.B. Quantum Computing Using Single Photons and the Zeno Effect. *Physical Review A*, 062302 (2004).

[6] Knill, E., Laflamme, R. & Milburn, G. A scheme for efficient quantum computation with linear optics *Supplementary Information*. *Nature* 409, 46–52 (2001)

[7] Shor, P. W. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A 52, R2493–R2496 (1995).

[8] Steane, A. M. Error Correcting Codes in Quantum Theory. Phys. Rev. Lett. 77, 793–797 (1996).

[9] J. Watrous, "On one-dimensional quantum cellular automata," Proceedings of IEEE 36th Annual Foundations of Computer Science, 1995, pp. 528-537

[10] P. Douglas Tougaw and Craig S. Lent , "Logical devices implemented using quantum cellular automata", Journal of Applied Physics 75, 1818-1825 (1994)

[11] E. Bernstein and U. Vazirani, Quantum Complexity Theory, Proc. 25^{th} Ann. ACM Symp. on Theory of Computing (1993) 11-20.

[12] Schumacher, B. Werner, R. F. Reversible quantum cellular automata. arXiv:quant-ph/0405174 (2004).

[13] T. Toffoli. Cellular Automata Mechanics. PhD thesis, University of Michigan, 1977.

[14] Perez-Delgado, C. A. & Cheung, D. Local Unitary Quantum Cellular Automata. Phys. Rev. A 76, 032320 (2007).

[15] Cheung, D. On Algorithms Separability and Cellular Automata in Quantum Computing. 140. (2007).

[16] Brennen, G. K. Williams, J. E. Entanglement dynamics in one-dimensional quantum cellular automata. Phys. Rev. A 68, 042311 (2003)

[17] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects.* Washington, DC: The National Academies Press.

[18] Luke Gordon, Justin R. Weber, Joel B. Varley, Anderson Janotti, David D.Awschalom, and Chris G.Van de Walle: *Quantum computing with defects.*

[19] D.B. Tretyakov, I.I. Beterov, V.M. Entin, and I.I. Ryabtsev, Institute of semiconductor physics, Siberian Division, Russian Academy of Sciences, Novosibirsk, Russia *Cold Atoms in Optical Lattices as Qubits for a Quantum Computer*

[20] Clarke, John; Braginski, Alex I, eds.(2006). *The SQUID HANDBOOK: Applications of SQUIDs and SQUID systems.*

[21] Devoret et al., QuantumInstitute.yale.edu. *Schrödinger Cats, Maxwell's Demon and Quantum Error Correction*

[22] Girvin Steve [NYU Physics], 2018 Apr 13. *Schrödinger Cats, Maxwell's Demon and Quantum Error Correction*. Youtube. https://www.youtube.com/watch?v=4NpTTw8d8zEt=876sab$_c$*hannel* = *NYUPhysics*

[23] Ryan Babbush , Jarrod R. McClean, Michael Newman, Craig Gidney, Sergio Boixo , and Hartmut Neven, 29 March 2021, *Focus beyond Quadratic speedups for Error-Corrected Quantum Advantage*

[24] Kadowaki, T.; Nishimori, H. (1998). *"Quantum annealing in the transverse Ising model"*. Phys. Rev. E. 58 (5): 5355. arXiv:cond-mat/9804280

[25] Tristan Zaborniak, Rogerio de sousa. *Benchmarking Hamiltonian Noise in the D-Wave Quantum Annealer.*

[26] Scarani, Valerio; Bechmann-Pasquinucci, Helle; Cerf, Nicolas J.; Dušek, Miloslav; Lütkenhaus, Norbert; Peev, Momtchil (29 September 2009), *The security of practical quantum key distribution.*

[27] Zhao, Yi (2009). *Quantum cryptography in real-life application: assumptions and security.*

[28] Reimer, Michael E.; Cher, Catherine (November 2019). *The quest for a perfect single-photon source.*

[29] mp, Martin; Höfling, Sven; Lu, Chao-Yang; Pan, Jian-Wei (2016). *On-demabd single photons with high etraction efficienca and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar*

[30] S.Kirkpatrick, C.D. Gelett and M.P. Vecchi, Science 220, 671 (1983) *Stocastic Relaxation, Gibbs Distributions, and the Bayesian Restoration of Images.*

[31] R.D. Somma, S. Boixo, and H. Barnum. Perimeter Institute for Theoretical Physics, Waterloo, ON N2L 2Y5, Canada. *Quantum Simulated Annealing.*

[32] Kadowaki, T.; Nishimori, H. (1998). *"Quantum annealing in the transverse Ising model"*. Phys. Rev. E. 58 (5): 5355. arXiv:cond-mat/9804280

[33] Theoretical condensed matter physics division and centre for applied mathematics and computational science, Saha institute of Nuclear Physics, Kolkata, India. *Quantum Annealing and Other Optimization Methods workshop, 2005.*