



MATHEMATICAL MODELLING OF QUANTUM COMPUTING

Arunabh Singh

Department of Electronics and Communications,
FET, MRIIRS, Faridabad, 121003, Haryana, India

Suraj Kumar Singh

Department of Electronics and Communications,
FET, MRIIRS, Faridabad, 121003, Haryana, India

Abstract - Quantum computing is a propitious technology which is likely to revolutionize computing. It differs from classical computing, in context of the algorithms it requires for computations and the methods of implementation which correspond to the principles of quantum mechanics. The clock frequency of existing computer processor systems may reach about 40 GHz within the next decade. By then one atom may represent one bit, but electrons under such conditions cannot be described by classical physics, due to this a new model of computing becomes absolutely inevitable. The prospect of quantum computing may have the potential in dealing with the problems faced by classical computing.

KEYWORDS: *Quantum computing, qubits, Bloch sphere, quantum register, Linear-optics, trapped ions, fibre optics, laser pulse shaping etc.*

I. INTRODUCTION

In accordance with the Moore's law which states that the number of the transistors in an integrated circuit (IC) doubles within every two years as the performance, efficiency and competence of computers keep improving with new technological developments, many researchers have arrived upon a more or less similar conclusion: the performance of the computer chips increases, while the size decreases exponentially over time. This growth is obviously flawed, the classical computing models used in the construction of current computers cease to be a work satisfactorily at atomic and subatomic levels. This is one of the most important reasons for the development quantum computing. Most of the challenges in the development of quantum computing mainly arise due to the complexity of quantum particles and their properties. Thus, this paper attempts to deliver some understanding of this highly interesting field of research. It should not be referred as an absolute guide to quantum computing, but as an introduction to

the subject, explaining the basics of quantum computers and an in-depth overview of some of the most important aspects of quantum computing, which includes linear optics, trapped ions and ultrafast laser pulse shaping

II. QUBITS

Bit is a fundamental unit of data in classical computing. The entire classical computing is based on definitive sequences of bits and their manipulations. Qubit being a quantum substitute plays a similar role in quantum computing. Suppose that we assume a bit of value 1. Relying on wherever the bit "resides" i.e. the hard drive or the processor we can conclude that there is a non-zero current through a wire or that a part of the hard drive is magnetized. Similarly, an electron might be measured having either an up spin or a down spin. Electrons having various other properties cannot be deemed as a bit.

Qubit is defined as a 2-dimensional complex vector, an element of C . Two base states are denoted as $|0\rangle$ and $|1\rangle$, and they are represented by base state vectors, $|0\rangle = [1, 0]$, and $|1\rangle = [0, 1]$, $|0\rangle, |1\rangle \in C^2$. Outcomes from the experiments in quantum physics tell us that quantum particles systems hardly behave discretely, instead they are superpositions of various possible states. Therefore, before measurement, qubit is in a superposition of $|0\rangle$ and $|1\rangle$. This means that any other qubit is a linear combination of base states, $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, with the constraint that $|\alpha|^2 + |\beta|^2 = 1$ {where for $\alpha = a + bi$, $a, b \in R$, $|\alpha| = \sqrt{a^2 + b^2}$ }. The standardized constraint is a result of the evaluation of α and β . $|\alpha|^2$ represents the probability of obtaining $|0\rangle$ when measuring our qubit and $|\beta|^2$, likewise, represents the probability of measuring $|1\rangle$. The $|\ast\rangle$ is called a qubit, and as was shown above, represents vectors, not just base state vectors. Basically for every $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the corresponding inverse vector is: $\langle\psi| = \alpha^\ast\langle 0| + \beta^\ast\langle 1| = [\alpha^\ast, \beta^\ast]$, or, more precisely, $\langle\psi| : C^2 \rightarrow C^2$, $\langle\psi|(x) = [\langle\psi|, X_i]$

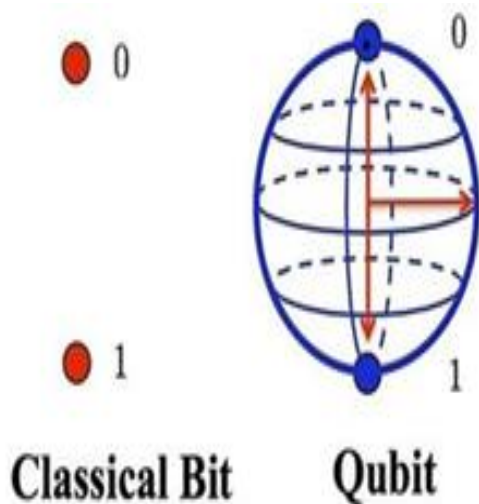


Figure 1: Bit vs Qubit

III. QUANTUM REGISTER

Generally, given two qubits x and y , since both x and y can be measured in two possible states, the quantum register containing only x and y has 4 possible states. We therefore denote the latest base states as $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, and all possible register states are linear combinations of these base states with complex coefficients. The two-qubit system is therefore constructed within C^4 . To accomplish that, we use the universal tensor product. To recap without the use of mathematical rigour, the tensor product from two 2-dimensional vector spaces is: $[x, y]^t \otimes [z, w]^t = [(x*z), (x*w), (y*z), (y*w)]^t$, and the general tensor product $\otimes : C(k) \times C(l) \rightarrow C(kl)$ is defined with:

$$v \otimes w = [v_1w \dots v_jw \dots v_kw], v \in C(k), w \in C(l),$$

where v_j is the j th component of vector v . $C(kl)$ can therefore, be constructed using the tensor product on the base vectors. It is obvious that our n -qubit system is contained in the vector space C^{2^n} . The definition of the tensor product is easily extended to matrices, which plays a vital role in constructing multi-qubit quantum gates. Using the tensor product, we can easily combine qubits into elements of the extended system. Indeed, $[|0\rangle, |1\rangle] \otimes [|0\rangle, |1\rangle]$ is the standard basis for C^4 , where $|0\rangle \otimes |0\rangle = |00\rangle, |1\rangle \otimes |0\rangle = |10\rangle$ etc., and similarly for an arbitrary quantum register. Since our quantum register also represents a quantum system and the amplitudes provide us with probabilities, it is obvious that we have to generalize the restriction regarding the amplitudes in a single qubit system i.e. the scale of our quantum register must be equal to 1. In other words, any given quantum register $|\psi\rangle = \alpha_1|00\dots0\rangle + \dots + \alpha_n|11\dots1\rangle$ must satisfy the equation $\sum_{k=1}^n |\alpha_k|^2 = 1$ where $|\alpha_k|^2$ is the probability of measuring the corresponding base state when measuring the entire quantum register.

IV. ENTANGLEMENT OF QUBITS

Consider a quantum register defined with $|\psi\rangle = 1/\sqrt{2} |01\rangle + 1/\sqrt{2} |10\rangle + 1/2 |00\rangle$. When measuring the first qubit of this quantum register, if the measurement gives us $|0\rangle$, the second qubit also collapses completely, since the only possible measurement result for the second qubit is obviously $|0\rangle$. On the other hand, were we to measure $|1\rangle$ on the first qubit, our quantum register would transform into $|\psi\rangle = 1/\sqrt{2} |10\rangle + 1/\sqrt{2} |11\rangle$, which, when measuring the second qubit, has the same probability of giving $|0\rangle$ and $|1\rangle$, while, originally, it was somewhat more probable to measure $|0\rangle$. We also had to resize the amplitudes to conserve the norm of our two-qubit register. Conversely, consider $|\phi\rangle = 1/2 |00\rangle + 1/2 |10\rangle + 1/2 |01\rangle + 1/2 |11\rangle$. It is evident that the result of any measurement of the state of the first qubit will not influence the results of measurement over the second qubit.

It can be easily shown that measurement over an individual qubit will not influence the remaining qubits if and only if the quantum register can be described as a multilinear aggregate of that qubit and the residual multi-qubit vector. When we take into consideration that measurement can change the properties of that system, we conclude that even a partial measurement can alter the behaviour of our quantum register. Thus, we can see that this effect corresponds to the physical effect of quantum entanglement. Indeed, this is our final explanation for the model. This generates the following classification: A multi-qubit state is entangled if it cannot be factorized into a product of specific qubits. Entanglement is a fascinating property because: given two or more entangled qubits, alterations regarding one qubit affect the entire register. This will play a crucial role in many quantum algorithms like Shor's algorithm and Grover's algorithm.

V. BLOCH SPHERE

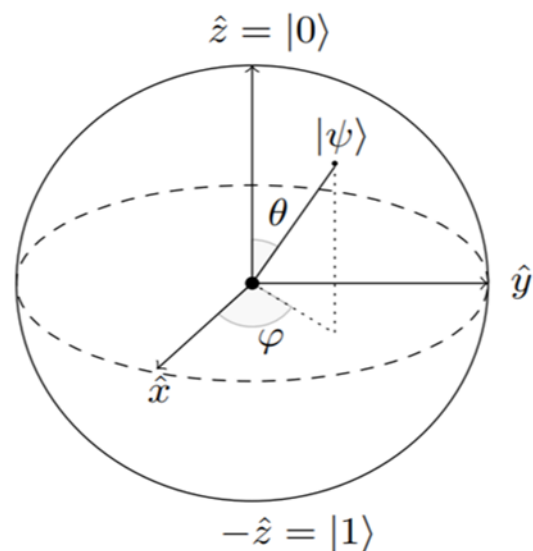


Figure 2: Bloch sphere

The Bloch sphere is a diagrammatic description of a qubit in its pure state in space, named after the physicist Felix Bloch. The Bloch sphere is a unit 2-sphere, with antipodal points equivalent to a pair of relatively orthogonal vectors. Both the poles of the Bloch sphere are specifically chosen to correspond to the universal base vectors $|0\rangle$ and $|1\rangle$ respectively, which in turn might correspond to the $(+1/2)$ and $(-1/2)$ states of an electron. This choice is subjective, however. The points on the surface of the sphere relate to the pure states of the system, although the inner points correspond to the mixed states. The Bloch sphere can be comprehensive to an n -level quantum system, but then the visualization is less effective. Given an orthogonal source, any pure state $|\psi\rangle$ of a two-level quantum system can be written as a superposition of the basis vectors $|0\rangle$ and $|1\rangle$, where the coefficient or quantity of each of the two base vectors is a complex number. This implies that the state is defined by four real digits. However only the comparative phase between the coefficients of the two base vectors has any tangible meaning, so that there is further inclusion in this description. We can take the coefficient of $|0\rangle$ to be real and non-negative. This permits the state to be defined by only three real numbers, enhancing the three-dimensional modelling of the Bloch sphere. As a result, the surface of the Bloch sphere signifies all the pure states of a qubit in space, whereas the core relates to all the mixed states. A valuable benefit of the Bloch sphere representation is that the development of the qubit state is explainable by rotations of the Bloch sphere. The most succinct explanation for why this is the case is that the linear algebra for the group of singular and Hermitian matrices (a complex square matrix equal to its own conjugate transpose) is isomorphic to the linear algebra of the group of three dimensional rotations. The set of all points on and inside the Bloch sphere is known as the Bloch ball.

VI. QUANTUM COMPUTING WITH LINEAR OPTICS

The major benefit of an optical methodology to quantum computing is that it could facilitate quantum logic gates and quantum memory devices to be easily connected together using optical fibres or wave guides in analogy with the wires of a compatible computer. This affords a type of modularity that is not readily available in other methods. For instance, the relocation of qubits from one location to another in trapped ion or NMR systems is a very challenging process. The major hindrance to an optical method has been the execution of the quantum logic gates required to perform calculations. An important example of a quantum logic gate is the controlled-NOT (CNOT) gate, which has been shown to be a universal gate for quantum computers in the same way that the typical NAND gate is a universal gate for classical computers. As described in reference, a CNOT gate has two inputs (a control qubit and a target qubit) and operates in such a way that the NOT operation is applied to the desired qubit, provided the control qubit has a rational value equivalent to 1.

Such a logic operation is intrinsically nonlinear because the state of one quantum particle must be capable of regulating the state of others. In an optical method, this is equivalent to lacking a nonlinear interaction between two distinct photons, which is typically an extremely weak effect. Though several effective methods for producing nonlinear interactions at single-photon intensity levels have been studied, they are assumed to be either inefficient or supplemented by too much loss to be of use to quantum CNOT gates. It has lately been shown, that near-perfect optical quantum logic gates, such as a CNOT gate, can be realized without the need for a nonlinear interaction between two distinct photons. Logic gates of this sort can be built using efficient linear optical elements, such as mirrors and beam splitters, supplementary reserved photons, and activating signals from single-photon detectors. In this “linear optics quantum computing” (LOQC) procedure, the inevitable non-linearity occurs from the quantum evaluation process regarding the detection of the additional reserved photons. Generally speaking, the resonant current of a single-photon detector can be switched on/off, which is done with the help of incident photons.

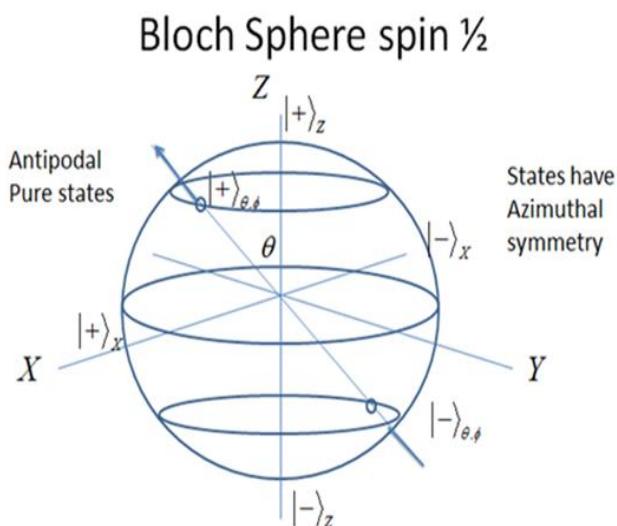


Figure 3: Spin states of a Bloch sphere

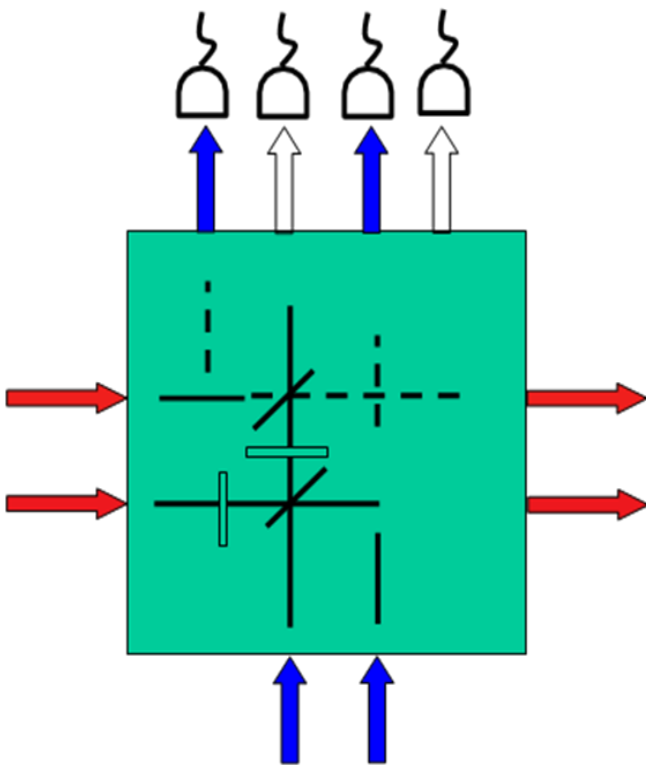


Figure 4: Two Input Quantum Logic gate using Linear Optics

The basic idea of a LOQC-type CNOT gate is illustrated in Figure 4. In addition to the control and target photons, the supplementary photons are inoculated into a “black-box” containing only linear optical components. The optics are designed in such a way that there are three types of outcomes from the device, each of which is signaled by a unique combination of triggering events at a series of single-photon detectors. In one set of outcomes, we can assume that the control and target photons are in the required logical output state. In the second type of outcome, the control and target are deduced to be in the wrong output state, but they can be rectified in a known way using real-time corrections known as feed-forward control. The third type of outcome suggests that the control and target photons have been missing, or they are in a logical state that cannot be rectified.

These LOQC logic gates are referred to as unpredictable devices because they sometimes fail, but we can detect when a failure has occurred. In addition, the gates can be designed in a certain way that the probability(P_f) of a failure event can be made capriciously small. According the initial LOQC scheme, it was deduced that P_f can be relative to $1/N$, where N is the number of ancilla photons utilized by the gate. An alternative approach in which P_f scales as $1/N^2$, which significantly decreases the amount of resources required for a given gate conformity. Fig 5 utilizes the entanglement of the ancilla

photons (photons operated by phase shifter) to execute the preferred quantum logic operation on the control and target qubits present at the input. The correct logical output is known to have been generated whenever each of the detectors transmit only one photon, which happens with a probability of $1/4$.

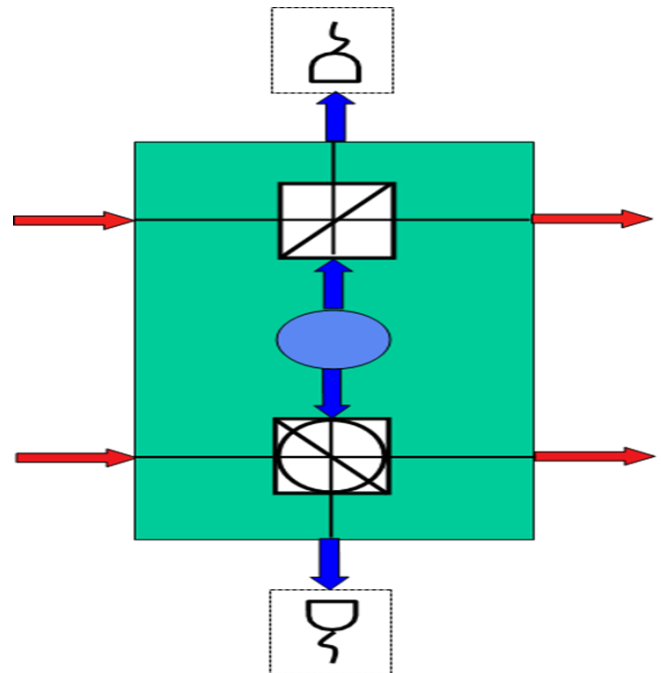


Figure 5: Linear Optical Quantum controlled NOT gate

The spontaneous parametric down conversion (SPDC) process is an instant optical process which involves passing an intense laser pulse through a non-linear medium because of which relative photons emerge infrequently. SPDC is a purely quantum-mechanical occurrence that can be viewed as the break-down of a relatively higher energy photon in an optical beam followed by the creation of two relatively lower energy photons, under the conditions that ensure conservation of energy and momentum. The functioning of CNOT logic gate with accuracy depends upon multi-photon quantum intrusion effects that necessitate the photons to be completely interchangeable, with an exception of their polarizations.

This requires a sequence of precise spectral filtering, the use of linear optical fibres for four-dimensional mode-matching, and timing accuracy on the order 10–13 seconds. Once these elements are optimized, the CNOT gate can be authenticated using polarizing optics to control the values of the control and target input qubits, and by using polarization analyzers followed by single-photon detectors to assess and evaluate the output of the device.

VII. QUANTUM COMPUTING WITH TRAPPED IONS

Quantum computing hardware has progressed rapidly in recent years. One of the most leading qubit technologies are trapped ion qubits. Trapped ions computers are built with large systems consisting of 11 qubits. All these systems have certain resource limitations, including low qubit values and high operative noise, and therefore are called Noisy Intermediate-Scale Quantum (NISQ) systems. In spite of these limitations, NISQ systems have the potential to demonstrate near-term Quantum computing applications especially if they are architected well and used in conjunction with efficient software “toolflows”.

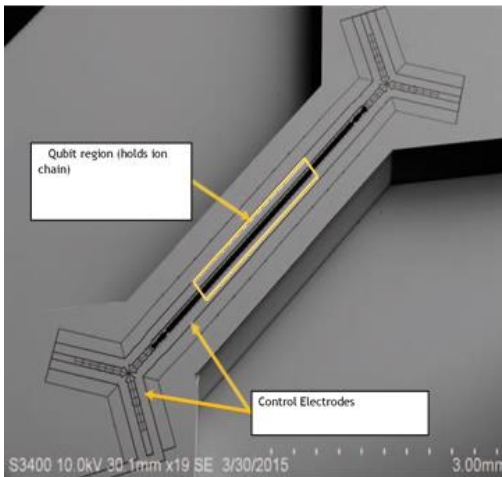


Figure 6: Scanning electron Micrograph

Trapped ion qubits are one the most promising technology candidates for building NISQ devices. Fig 6 shows a real Trapped ions Quantum Computing system. Trapped Ion qubits are implemented using the energy states of an atomic ion such as Ca^+ or Yb^+ . In a Trapped ion system, a set of ions are trapped or confined in space using electromagnetic fields.

As Figure 7a shows, the ions are arranged in the form of a linear chain, with each ion storing a single qubit. The states of the ions can be manipulated using lasers to implement gate based computation. Current Trapped ions systems with 5-11 qubits have been used to demonstrate near-term applications and quantum error detection. Although they are less efficient than linear optical devices like CNOT gate they have structural advantages over other technologies, including perfectly identical qubits, very high coherence times and dense qubit connectivity. Indeed, recently advance research has revealed various ways in which Trapped ion systems perform better than superconducting systems of the same size.

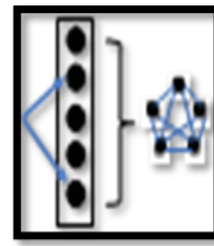


Figure 7a: 5-Qubit system with single trap

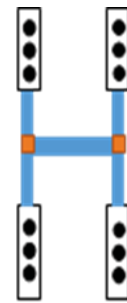


Figure 7b: Molecular QCCD system

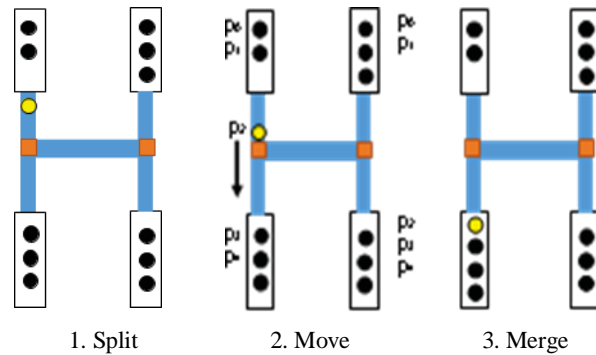


Figure 7c: Shuttling operation on p_2

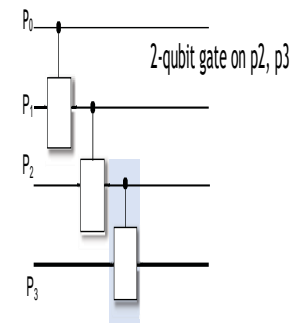


Figure 7d: Example program of IR

Fig 7a shows 5-qubit Trapped ion system with a single trap. Each black circle represents a qubit. Multi-qubit gates are accomplished by pulsing the required pair of qubits with lasers, permitting a single trap to sustain full connectivity among the qubits. Fig 6b shows modular Quantum Charge Coupled Device (QCCD) with 4 traps. QCCD was proposed to make long ion chain technology consisting of 50-100 qubit systems feasible. Each trap initially has 3 ions and a maximum capacity of 4 ions. The traps are interconnected through shuttling paths to move ions from one trap to another. The orange squares represent junctions where shuttling paths meet. Fig 7d represents an example of program intermediate representation (IR). For



clarity, we show only two-qubit gates. Real program IR also comprises of single-qubit gates and qubit evaluation procedures. To execute the IR on the device in fig 7a, each ion in the device can be used to represent one qubit from the IR, and gates can be executed using the laser controller. In fig 7c (to execute the IR on the device in fig 7b) P0, P1 and P2 are mapped onto one trap, and P3 and P4 are mapped onto another. The first two gates are executed within the top left trap. For the gate on P2 and P3, the qubits need to be relocated within the same trap, so P2 is shuttled to the trap containing P3 and the gate is performed inside the bottom left trap. QCCD-based Trapped ion systems use several traps, with each trap possessing a small quantity of ions, allowing steady gates and full connectivity within each trap. In order to combine traps, QCCD systems use ion shuttling, where qubits are tangibly moved so as to ease communication between traps. While several other scaling proposals exist in theory, all basic components required for QCCD systems have been developed and refined over the last decade, making it a very promising Trapped ion scaling path.

VIII. CONCLUSION

Today's feasible quantum computer is based on seven-bit NMR, which can factorize up to 15 digit numbers. Further research is necessary, through persistent evaluation of quantum computing using classical computers. Simulators must be able to handle quantum computers that operate on a practically large number of qubits. Thus, we need to employ large-scale parallel processing methods to acquire more meaningful results within a given time frame. By relating the basic concepts of classical computing such as hardware extraction to quantum computing, the progress in research can be accelerated. Efforts made by researchers to understand the correlation between quantum mechanics and computing have hardly commenced. Undoubtedly, we need more extensive research in the physical realization of components of quantum computers. Computer scientists and engineers will need to consider the various architectural solutions for quantum computing as well as the various latest quantum algorithms to enhance the functioning of quantum computers. Over the last two decades, all components required for QCCD systems have been experimentally developed and perfected. However, building a practically useful QCCD system is difficult due to the wide range of possible hardware choices and the need to support advancements in Quantum computing applications. A linear optics approach appears to be the most promising methodology for accommodating large scale applications of quantum computing.

IX. REFERENCES

[1] Feynman R.P., "Quantum mechanical computers", 1985, *Optical News* 11, (pp.11-20).

[2] Monroe R. Christopher, 2002, "Quantum Information Processing with Atoms and Photons.", *Nature*, Vol. 416, No. 6877, (pp. 238–246).

[3] Franson J.D. and Jacobs B.C., 1997, "Quantum Computing", *Johns Hopkins APL Tech.*, (pp.188-192).

[4] Monroe C., Meekhof D.M., King B.E., Itano W. and Wineland D.J., 1995, "Demonstration of a Fundamental Quantum Logic Gate", *Phys. Rev. Lett.* 75, (pp. 4714-4717).

[5] Ahn J., Weinacht T.C. and Bucksbaum P.H., 2000, *Science*, Vol.287, (pp.463-478).

[6] Goswami D., 2003, *Physics Reports*, Vol. 374, (pp. 385-416).

[7] Wang X., Sørensen A., Mølmer K., 2001, "Multibit gates for quantum computing." *Phys. Rev. Lett.*, (pp.3907–3910).

[8] Weber E. W., 1977, "Optical pumping of ions.", *Phys. Rev.* 32, (pp.123).

[9] DiVincenzo D.P., 2000, "The physical implementation of quantum computation", *Fortschritte der Physik*, (pp. 771–783).

[10] World's first universal quantum computation simulator, Quantum computer simulator, SENKO Corporation, <http://www.senko-corp.co.jp/qcs/index.html>.

[11] Franson J.D., 1997, "Cooperative Enhancement of Optical Quantum Gates", *Phys. Rev. Lett.* 78, (pp.3852-3855).

[12] Knill E., LaFlamme R. and Milburn G.J., 2001, "A scheme for efficient quantum computation with linear optics", *Nature* 409, (pp. 46-52).

[13] Walmsley I. A., 2008, "Looking to the future of quantum optics." *Science* 319, (pp. 1211-1234).

[14] Shor P.W., 1996, "Fault-tolerant quantum computation", *Proc. 37th IEEE Annual Symp. on Foundations of Computer Science*, (pp. 56–65).

[15] Cirac J.I. and Zoller P., 1995 "Quantum computations with cold trapped Ions", *Physical Review Letters*, (pp. 4091-4111).

[16] Einstein, A., Podolsky, B., and Rosen, N., 1935, "Can Quantum Mechanical Description of Physical Reality be Considered Complete?", *Phys. Rev.* 48, (pp. 696-702).

[17] Selinger P., 2003, "Towards a quantum programming language, *Mathematical Structures in Computer Science*", (pp. 527-546).