Analysis and Review of Mathematical Concepts in Quantum Computation

M. A. Bashar, Mahmudul Hasan
Department of Computer Science and Engineering,Comilla University, Comilla, Bangladesh
E-mail: {basharcse, mhasanraju}@gmail.com

M. A. Chowdhury, M. Syduzzaman
Therap Services LLC, Dhaka, Bangladesh
E-mail: {misbahulalam, syduzzaman.cse}@gmail.com

Abstract
The basic principle behind quantum computation is that quantum properties can be used to represent data and perform operations on these data. Mathematics lies at the heart of quantum computation and it is needed in every aspect of the research and development of quantum computation. In this paper we have presented mathematical concepts that are closely related to quantum computation and their relation to quantum mechanics in a way which is innovative and very easy to comprehend. Most of the mathematical concepts presented in this paper are deduced from the postulates of quantum mechanics and linear algebra.
Keywords: Quantum computation, quantum mathematics, quantum gate, quantum operator, reversible computing, parallel computing.

1. Introduction

In the classical model of a computer, the most fundamental building block, the bit, can only exist in one of two distinct states, a 0 or a 1. In a quantum computer the rules are changed. Not only can a 'quantum bit', usually referred to as a 'qubit', exist in the classical 0 and 1 states, it can also be in a coherent superposition of both. When a qubit is in this state it can be thought of as existing in two universes, as a 0 in one universe and as a 1 in the other. An operation on such a qubit effectively acts on both values at the same time. The significant point being that by performing the single operation on the qubit, the operation has been performed on two different values. Likewise, a two-qubit system would perform the operation on 4 values, and a three-qubit system on eight. Increasing the number of qubits therefore exponentially increases the 'quantum parallelism' we can obtain with the system. With the correct type of algorithm it is possible to use this parallelism to solve certain problems in a fraction of the time taken by a classical computer [1, 2].

The discovery made by Shor [3, 4] that computation with quantum states instead of classical bits can result in large savings in computation time has made a breakthrough in the regime of quantum computation. It is estimated that a quantum computer using 36 qubits could very quickly perform computations that would require a conventional computer 13 billion years to perform. It has shown that quantum computer can speed up exponentially. Though quantum computer is not in our hand but the recent research makes us to hope that it is steeping in. To understand and utilize the quantum computation we need some basic mathematical concepts relating state space of the computation system, transformation of one computational state to another, measuring the state to get the computational output and combined computational state space system. In this paper we have presented these in an innovative and straightforward manner which is very easy to understand. We have also described the mathematical concepts of superposition and parallel computation using Dirac's bra-ket notation. The matrix operations introduced here obey the laws of linear algebra [5, 6, 7].

2. Linear Algebra

The linear algebra terms that are most frequently used in quantum computation are the following –

Basis: In linear algebra, a basis is a set of linearly independent vectors that, in a linear combination, can represent every vector in a given vector space.

Linearly independent: In linear algebra, a family of vectors is linearly independent if none of them can be written as a linear combination of finitely many other vectors in the collection.

Z^* - complex conjugate

if $Z = a + b.i$ then $Z^* = a - b.i$

$|\Psi\rangle$ - vector, "ket" i.e.

$$\begin{bmatrix} C_1 \\ C_2 \\ \dots \\ C_n \end{bmatrix}$$

$\langle \Psi|$ - vector, "bra" i.e.

$$[C_1^*, C_2^*, \ldots, C_n^*]$$

$\langle \varphi|\Psi\rangle$ - inner product between vector $\langle \varphi|$ and $|\Psi\rangle$.

Note $\langle \varphi|\Psi\rangle = \langle \Psi|\varphi\rangle^*$

Example: $|\varphi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix}$, $|\Psi\rangle = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$

$$\langle \varphi|\Psi\rangle = [2, -6i] \begin{bmatrix} 3 \\ 4 \end{bmatrix} = [6 - 24i]$$

$|\varphi\rangle \otimes |\Psi\rangle$ tensor product of $|\varphi\rangle$ and $|\Psi\rangle$.

Also written as $|\varphi\rangle|\Psi\rangle$

$$\text{Example: } |\varphi\rangle|\Psi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix} \otimes \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \times 3 \\ 2 \times 4 \\ 6i \times 3 \\ 6i \times 4 \end{bmatrix} = \begin{bmatrix} 6 \\ 8 \\ 18i \\ 24i \end{bmatrix}$$

A^* - complex conjugate of matrix A.

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^* = \begin{bmatrix} 1 & -6i \\ -3i & 2-4i \end{bmatrix}$$

A^T - transpose of matrix A.

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^T = \begin{bmatrix} 1 & 3i \\ 6i & 2+4i \end{bmatrix}$$

$A^\dagger$- Hermitian conjugate (adjoint) of matrix A.

Note $A^\dagger = (A^T)^*$

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^\dagger = \begin{bmatrix} 1 & -3i \\ -6i & 2-4i \end{bmatrix}$$

$\| |\Psi\rangle \|$ - norm of vector $|\Psi\rangle$

$$\| |\Psi\rangle \| = \sqrt{\langle \Psi|\Psi\rangle}$$

Important for normalization of $|\Psi\rangle$ i.e. $|\Psi\rangle / \| |\Psi\rangle \|$

$\langle \varphi|A|\Psi\rangle$ – inner product of $|\varphi\rangle$ and $A|\Psi\rangle$.

or inner product of $A^\dagger$ and $|\Psi\rangle$

3. Mathematical Analysis of Quantum Computation based on Quantum Postulates

3.1. Postulate 1

Associated to any isolated physical system is a complex vector space with inner product known as the state space (Hilbert space) of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

3.1.1. State Space

One of the basic notions for the description of a physical system is that of its 'state'. The 'state' of a physical system essentially can then be defined, roughly, as the description of all the known properties of that system and it therefore represents our knowledge about this system. In physics, a quantum state or state vector is a set of mathematical variables that fully describes a quantum system. The set of all states forms what we usually call the state space. Quantum mechanical state space differs from that of classical mechanics. One reason for this can be found in the ability of quantum systems to exist in coherent superpositions of states with complex amplitudes, other differences relate to the description of multi-particle systems. This suggests, that a good choice for the quantum mechanical state space is a complex vector space [8]. The basis states of the Hilbert Space define the state of a Quantum System. Simplest quantum system is the Q-bit that can be described by the state vector $|\Psi\rangle$ [9, 10, 11]. The basis states for a Q-bit are written as two dimensional state space $|0\rangle$ and $|1\rangle$, then the state vector for the Q-bit is:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

where α and β are complex numbers with α2 + β2 = 1. This equation discloses that $|\Psi\rangle$ is a unit vector that is is $\langle\Psi|\Psi\rangle = 1$ and this condition is often known as the normalization condition. Instead of $|0\rangle$ and $|1\rangle$ we can use any other basis states, as long as we can distinguish evidently between the two. Mathematically, basis states must be the orthogonal vectors. That's why in two-dimensional Hilbert Space:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, |\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \qquad (2)$$

In Quantum computation, information is stored in the Q-bit. From the above matrix formulation we have, if $\alpha = 0$, then $|\Psi\rangle = |1\rangle$ and oppositely, if $\beta = 0$, then $|\Psi\rangle = |0\rangle$ which are same as the classic computing bits. So the superposition of $|0\rangle$ and $|1\rangle$ that is $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ which gives us the golden opportunity to store them simultaneously. Hence true parallelism in processing information can be obtained about which we discuss at the end.

3.2. Postulate 2

The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\Psi(t_1)\rangle$ of the system at time t1 is related to the state $|\Psi(t_2)\rangle$ of the system at time t2 by a unitary operator U which depends only on times t1 and t2.

That is $|\Psi(t_2)\rangle = U(t1,t2)\,|\Psi(t_1)\rangle$, $U^\dagger U = 1$.

3.2.1. Quantum Operators and Evolution

The process of the change of the state $|\Psi\rangle$ of a closed quantum mechanical system with time is evolution. This is the information processing way in quantum computation. So, the unitary operators of quantum mechanics as the quantum gates for quantum computation [12]. A quantum gate is represented by a two dimensional matrix, which may be applied on the information of Q-bit with state $|\Psi\rangle$ for computation. Let's look at a few instances of quantum gates on a single Q-bit, which are central in quantum computation:

- The Pauli gates (X, Y, Z, I)
- The Hadamard gate (H)
- Controlled NOT Operator (cNot)

i. Bit flip: $X: X(\alpha|0\rangle + \beta|1\rangle) \equiv \alpha|1\rangle + \beta|0\rangle$ (3)

Where, $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

ii. Phase Shift and Bit Flip:

$Y: Y(\alpha|0\rangle + \beta|1\rangle) \equiv i(\alpha|1\rangle - \beta|0\rangle)$ (4)

Where, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

iii. Phase Shift: $Z: Z(\alpha|0\rangle + \beta|1\rangle) \equiv \alpha|0\rangle - \beta|1\rangle$ (5)

Where, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

iv. Identity: $I: I(|x\rangle) \equiv |x\rangle$ (6)

Where, $I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

v. Hadamard gate (H):

Before going to Hadamard operator we should be introduced with the operators n, $\bar{n}$, and Z**.**

The operator n and $\bar{\boldsymbol{n}}$ is defined as,

$$n \leftrightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \bar{n} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad (7)$$

Then we get the operator Z which is defined as,

$$Z = \bar{n} - n \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (8)$$

Now using Z and X we can get the Operator Hadamard which is specified as,

$$H = \frac{1}{\sqrt{2}}(X + Z) \leftrightarrow \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (9)$$

Like X gate we can also get for the Hadamard gate that $H^2 = HH = 1$

When H is applied on $|0\rangle$ and $|1\rangle$ then we get,

$$H|0\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle), H|1\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \quad (10)$$

If we take $|0\rangle|0\rangle$ as initial state for two Q-bit and apply H operator then we get the following,

$$(H \otimes H)(|0\rangle|0\rangle) = (H|0\rangle)(H|0\rangle)$$
$$= \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)\frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)$$
$$= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1|0\rangle + |1\rangle|1\rangle)$$
$$= \frac{1}{2}\left(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2\right) \quad (11)$$

So we became able to convert a 2 bit basis state $|0\rangle|0\rangle$ to an equally weighted superposition of all possible 2 q-bit inputs.

If we generalize this concept then using the n-fold tensor product of **n** Hadamard transforms ($H^{\otimes n}$), we can get

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}}\sum_{0 \le x < 2^n}|x\rangle_n \quad (12)$$

Thus we got the equally weighted superposition of all possible **n** q-bit inputs. This superposition is ready for parallelism. Now if we have a good algorithm for utilizing parallelism then you are getting this state of n q-bit appropriate for your goal.

Quantum computation allows true parallel computing and its parallelism increases with the number of Q-bits. Quantum Parallelism is the fundamental feature of many quantum algorithms (i.e. Peter Shor's factorizing, and

Grover's search algorithm). Heuristically, quantum parallelism allows quantum computers to evaluate a function f(x) for many different values of x simultaneously. Parallel evaluation of a function with an n Q-bits input x and 1 Q-bit output, f(x) can be performed in the following manner [13]:

1. Prepare the n+1 Q-bits state as $|0\rangle^{\oplus n}|0\rangle$.
2. Apply the Hadamard gate to the first n Q-bits.
3. Apply quantum unitary gate U_f to perform f(x). For all possible values of |x⟩ outcome |f(x)⟩ will be stored in (n+1)th Q-bit. The consequent is an astonishing state in the sense that it is almost as if we have evaluated f(x) for all possible values of x simultaneously admitting the power of quantum computation.
4. Measuring the final state with respect to the computational basis we will obtain only one output rather than all with arbitrary probability.

The above four are the principle steps for computation in the quantum computer.

vi. Controlled NOT Operator (cNOT):

The controlled NOT operator (cNOT) is an extremely important operator in quantum computation [14]. This operator C_{ij} operates on two bits where i-th bit is known as control bit and j-th bit is known as target bit. If i-th bit is 0 the C_{ij} does not change j-th bit otherwise flips the j-th bit. In both cases the i-th bit remains unchanged. So, we can define C_{ij} as

$$C_{ij}|x\rangle_1|y\rangle_1 = |x\rangle_1|y \oplus x\rangle_1, \text{ and the corresponding matrix is } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

That is, $|00\rangle \longrightarrow cNOT \longrightarrow |00\rangle$ and $|11\rangle \rightarrow cNOT \rightarrow |10\rangle$

Any arithmetical operation on bits can be carried out on basis with operations built up out of 1 q-bit gates acting in suitable combination with 2 q-bit cNOT gate [4]. Other operators can be designed for some algorithm design when necessary.

Controlled-NOT or CNOT gate is the prototypical multi Q-bits reversible quantum logic gate. Execution of a quantum algorithm, on a quantum computer, means the unitary evolution of the states of the quantum system. All unitary operators U obey the rule: $(U^T)^* = U^{-1}$. That means it is always possible to "uncompute" (reverse) a computation on a quantum computer. Landauer (in 1961) showed that almost all computational operations can be done in a reversible way. When a device can actually run backwards it is called physically reversible. Thus quantum computation is reversible, and according to the second law of thermodynamics it dissipates no heat [15, 13].

3.3. Postulate 3

Quantum measurements are described by a collection {Mm} of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\Psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle \Psi | M_m^\dagger M_m | \Psi \rangle$$

and the state of the system after the measurement is

$$\frac{M_m|\Psi\rangle}{\sqrt{\langle \Psi | M_m^\dagger M_m | \Psi \rangle}}$$

The measurement operators satisfy the completeness equation –

$$\sum_M M_m^\dagger M_m = I$$

The completeness equation expresses the fact that probabilities sum to one –

$$1 = \sum_M p(m) = \sum_M \langle \Psi | M_m^\dagger M_m | \Psi \rangle = I$$

3.3.1. Explanation of Quantum Measurements

Measurement is viewed in different ways in the many interpretations of quantum mechanics; however, despite the considerable philosophical differences, they almost universally agree on the practical question of what results from a routine quantum-physics laboratory measurement. To describe this, a simple framework to use is the Copenhagen interpretation, the utility of this approach has been verified countless times, and all other interpretations are necessarily constructed so as to give the same quantitative predictions as this in almost every case [16]. Before we took our measurement the wavefunction could have been anything that is we have no idea what the wavefunction was before we took the measurement. Measuring causes its wavefunction to become an eigenstate of whatever (e.g., momentum, position) we chose to measure. For example, a physical system - such as an electron - exists partly in all its particular, theoretically possible states (or, configuration of its properties) simultaneously; but, when measured, it gives a result corresponding to only one of the possible configurations [17].

In their paper Gary Felder et al. [6] describes that in classical mechanics we know that if we measure the position and momentum of a particle two times in a row we should get the same result both times, but if we wait an hour in between the two measurements we expect to get different answers. Specifically, the way the state of the particle changes is determined by Newton's second law F=ma. In quantum mechanics the situation is very similar. Once we measure something about our particle we know its state, i.e. its wavefunction. If we wait for a while that wavefunction will evolve. Once again that evolution is determined by a differential equation, which in quantum mechanics is called Schrödinger's equation. Mathematically the analogy between Schrödinger's equation and F=ma are the following –

Newton's Second Law is a second-order differential equation, $F = m\frac{d^2x}{dt^2}$. If you know the forces acting on a particle, you can solve this equation to find x. However, your solution will have two arbitrary constants, corresponding to the position and velocity at time t=0. If you plug in those two constants, you get a specific function x(t) (and its derivative v(t)). This is the mathematical equivalent of the physical principle we stated earlier—given the forces and a measurement at a particular time, you can predict the state of the particle in the future.

Schrödinger's equation is a mixed-order *partial* differential equation, meaning the function you are solving for (Y) depends on two variables (x and t). If you know the potential energy function V(x), you can solve this equation to find Y. However, your solution will have an *arbitrary function,* which corresponds to the function Y(x) at t=0. If you plug in that function, you get a specific function **Y**(x,t). This is the mathematical equivalent of the physical principle we stated earlier—given the potential energy function and a measurement at a particular time, you can predict the state of the particle in the future.

An example given in [13] describes that if we do the measurement of a Q-bit with state $|\Psi\rangle$ there are two possible outcomes either $|0\rangle$ or $|1\rangle$. If the measurement is done with respect to the $\{|0\rangle, |1\rangle\}$ basis, the following situations can arise [4, 3]:

a) If $|\Psi\rangle = |0\rangle$, the answer will be $|0\rangle$ with probability 100%.
b) If $|\Psi\rangle = |1\rangle$, the answer will be $|1\rangle$ with probability 100%.
c) In all other cases (e.g. $\alpha^2=\beta^2=0.5$), the result will be probabilistic.

After measurement, the previous state of $|\Psi\rangle$ will convert to the result obtained permanently. We may obtain this result mathematically [3] by considering two measurement operators $M_o= |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Observe that each measurement operator is Hermitian, and that $M_0^2 = M_0$, $M_1^2 = M_1$. Thus the completeness relation is obeyed:

$$I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1 \tag{13}$$

Then the probability of obtaining measurement outcome $|\mathbf{0}\rangle$ is –

$$p(|0\rangle) = \langle\Psi|M_0 \dagger M_0|\Psi\rangle = \langle\Psi|M_0|\Psi\rangle = |\alpha|^2 \tag{14}$$

Similarly, we have - $p(|1\rangle) = |\beta|^2$ (15)

The state after measurement in these two cases is therefore:

$$\frac{M_0|\Psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle, and\ \frac{M_1|\Psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle \tag{16}$$

If we use a different measurement basis, the result will be one of the basis states, with different probabilities.

If we have a random quantum system and we measure it, we immediately know the basis state in which the system is after the measurement. Now, we can change this state to any other basis by just flipping the corresponding q-bits using operators. Even we can create an equally weighed superposition of all possible basis states using Hadamard operator. So, measurement may act to initialize the system and to know the final output [14].

3.4. Postulate 4

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and the system number i is prepared in the state $|\Psi_i\rangle$ then the joint state of the total system is

$$|\Psi\rangle = |\Psi 1\rangle \otimes |\Psi 2\rangle \otimes |\Psi 3\rangle \otimes \ldots . . \otimes |\Psi n\rangle.$$

3.4.1. How Composite Systems work

Two or more distinct physical systems represented by corresponding Q-bits can make a composite system. The state space of each component of the system builds the state space of composite system. The state of a composite quantum system $|\Psi\rangle$, with n Q-bits is their tensor product [3][4]:

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle \otimes |\Psi_3\rangle \otimes \ldots . . \otimes |\Psi_n\rangle \tag{23}$$

The tensor product for two Q-bits can be given as:

$$\Psi_1 \otimes \Psi_2 = \begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix} \otimes \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} = \begin{pmatrix}\alpha_0\alpha_1\\ \alpha_0\beta_1\\ \beta_0\alpha_1\\ \beta_0\beta_1\end{pmatrix} = \begin{pmatrix}\delta_{00}\\ \delta_{01}\\ \delta_{10}\\ \delta_{11}\end{pmatrix} \quad (24)$$

Here, two Q-bits system results in 4 basis states and we will get an arbitrary superposition of those Q-bits [17]. So for n Q-bits there will be 2^n basis states. Hence, the dimensionality of the Hilbert Space grows exponentially with the size of the n.

Let us we want to know the possible outcomes of measuring the two Q-bits state:

$$\Psi = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$
$$= \underline{\alpha\gamma|00\rangle + \alpha\delta|01\rangle} + \underline{\beta\gamma|10\rangle + \beta\delta|11\rangle} \quad (25)$$

Then, first measurement reduces $|\Psi\rangle$ to one of these underlined smaller states, with probability-prob. $|\alpha\gamma|^2 + |\alpha\delta|^2$, and prob. $|\beta\gamma|^2 + |\beta\delta|^2$. The second measurement reduces $|\Psi\rangle$ to one of the four states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ with probabilities $|\alpha\gamma|^2$, $|\alpha\delta|^2$, $|\beta\delta|^2$, and $|\beta\delta|^2$ in due order.

4. Conclusion

We have done the analysis and review of basic mathematical concepts that highlight the whole process of quantum computation. Mathematical concepts that are presented in this paper are the building blocks of designing quantum algorithms. Quantum computational process starts with a known basis then changes it to a superposition state after that, apply the necessary operations on it to evolve the quantum state and finally get the output by measurement. It is algorithm designer's responsibility to define the way of taking different decisions from the output of the process. The challenging task of an algorithm designer is to collapse the superposition using measurement to a basis state which is analogous to the considered algorithm. Concepts presented in this paper will also help to comprehend teleportation which is a new and exciting filed of future communication.

References

[1] Quantum Computer. http://en.wikipedia.org/wiki/Quantum_computer.
[2] Marius N. and Selim (2006), G. A., "Quantum Computation and Quantum Information." The International Journal of Parallel, Emergent and Distributed Systems, 21(1):1-59.
[3] Shor, P. W. (1994), "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." Proceeding of 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, pp. 124-134.
[4] Shor, P. W. (1997), "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. on Computing, 26(5):1484-1509.
[5] Nielson, M. A. and Chuang, I. L. (2003), *Quantum Computation and Quantum Information*, Cambridge University Press, Reprinted 2003, Chapter 1, 2, 4.
[6] Mermin, N. D. (2004), *Lecture Notes on Quantum Computation*, Cornell University.
[7] Liboff, R. L., *Introductory Quantum Mechanics*, Fourth Ed., Pearson Education.
[8] Martin Pleni, "Quantum Mechanics," Imperial College, Lecture, Version January 28, 2002
[9] Rahman, S. M. (2000), "Quantum Computation," Proceeding of International Conference on Computer and Information Technology, Dhaka, Bangladesh.
[10] A Short Introduction to Quantum Computation. http://www.qubit.org/library/intros /comp/comp.html.
[11] Barenco, A., Bennett, C. H., Cleve, R., DiVicenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. and Weinfurter, H. (1995), "Elementary Gates for Quantum Computation." Physical Review A, 52(5):3457-3467.
[12] Md. Towhidul Islam Talukder, Md. Ruhul Amin, Shahidul Islam, Chandan Kumar Karmakar, "Quantum Mechanics: The Driving Wheel of Quantum Computation," SUST STUDIES, Vol. 7, 2007, Journal of Shah Jalal University of Science & Technology, Sylhet, Bangladesh.
[13] Peres, A. (1085), "Reversible Logic and Quantum Computers," Physical Review A, 32(6):3266-3276.
[14] Md. Towhidul Islam Talukder, Md. Ruhul Amin, Shahidul Islam, "Designing Algorithms in Quantum Computation", Shah Jalal University of Science and Technology, B.Sc. Engg. thesis, Submission date 27th April 2007.
[15]Landauer, R. (1961), "Irreversibility and Heat Generation in the Computing Process," IBM Journal of Research and Development, 5(3):183-191.
[16] Available at: http://en.wikipedia.org/wiki/Quantum_measurement
[17] Available at: http://en.wikipedia.org/wiki/Quantum_superposition