UITS Journal Volume: 4 Issue: 2
ISSN : 2226-3128

A Brief Study on Quantum Computation

Goutam Paul[1]

Abstract

Quantum Computing is a very emerging field. Computing devices that we use right now are called classical computers because they follow the laws of classical physics. On the other hand, quantum computers work under the laws of quantum physics. Theoretically, Quantum computers are exponentially faster than classical computers. An understanding of some basic features of quantum mechanics is mandatory for any beginner in the field of quantum computation.

Keywords: *Qubit, Hilbert space, Bra-ket notation, Entanglement.*

INTRODUCTION

Quantum Computing is the art of using all the possibilities that the laws of quantum mechanics give us to solve computational problems. Classical Computers only use a small subset of these possibilities. In essence, they compute in the same way that people compute by hand. As a result, the class of problems that can be solved efficiently is the same as the class that can be solved efficiently by hand. In Quantum Computing, calculations are performed by unitary transformations on the state of the qubits combined with the principle of superposition. This creates possibilities that are not available for hand calculations. Quantum physics or quantum mechanics governs the world of elementary particles such as electrons and photons, and it is paradoxical, unintuitive, and radically strange.

1. BACKGROUND

The story of quantum computation started as early as 1982, when the physicist Richard Feynman considered simulation of quantum-mechanical objects by other quantum systems. Feynman observed that that certain quantum mechanical effects cannot be simulated efficiently on a classical computer. This observation led to speculation that perhaps computation in general could be done more efficiently if it made use of these quantum effects [3]. However, the unusual power of quantum computation was not really anticipated until 1985 when David Deutsch of the University of Oxford published a crucial theoretical paper in which he described a universal quantum computer [5]. But building quantum computers, computational machines that use such quantum effects proved tricky, and as no one was sure how to use the quantum effects to speed up computation,

[1] Lecturer, Northern University Bangladesh, Dhaka, Bangladesh, E-mail: goutampaul21@yahoo.com

the field developed slowly. It wasn't until 1994, when Peter Shor surprised the world by describing a polynomial time quantum algorithm for factoring integers [6], that the field of quantum computing came into its own. This discovery prompted a flurry of activity, both among experimentalists trying to build quantum computers and theoreticians trying to find other quantum algorithms.

2. MOTIVATION FOR QUANTUM COMPUTING

During last fifty years, manufacturing of computers has gone through outstanding development. The number of atoms needed to represent a bit in memory has been decreasing exponentially since 1950. Moreover, the number of transistors per chip doubled every 18 months, towards the direction of Moore's law. But this rate of improvement can't be sustained much longer. At the current rate, in the year 2020, one bit of information will require one atom to represent it. At that size, the behaviour of computer's components will not be dominated by classical physics, rather by quantum physics [1]. This physical limitation of classical computer and the possibility that the quantum computer can perform certain tasks more efficiently than classical computers drive the study of quantum computing. The most fundamental building block of a classical computer is the bit. A bit is capable of storing one piece of information; it can have a value of either 0 or 1. In a classical computer, a bit is typically stored in a silicon chip, or on a metal hard drive platter, or on a magnetic tape. About 10^{10} atoms are typically used to store one bit of information [8]. The smallest conceivable storage for a bit involves a single elementary particle of some sort. For example, any particle with a spin-1/2 characteristic can be characterized by its spin value, which when measured is either +1/2 or −1/2. We can thus encode 1 to be +1/2 and 0 to be −1/2, and if we assume we can measure and manipulate the spin of such a particle then we could theoretically use this particle to store one bit of information. If we were to try to use this spin−1/2 particle as a classical bit, one that is always in the 0 or 1 state, we would fail. We would be trying to apply classical physics on a scale where it simply is not applicable. This single spin −1/2 particle will instead act in a quantum manner [1]. Quantum computers are so powerful for special feature called quantum parallelism. Classically, the time it takes to do certain computations can be decreased by using parallel processors. To achieve an exponential decrease in time requires an exponential increase in the number of processors, and hence an exponential increase in the amount of physical space needed. However, in quantum systems the amount of parallelism increases exponentially with the size of the system. Thus, an exponential increase in parallelism requires only a linear increase in the amount of physical space needed. This effect is called quantum parallelism [7].

3. AXIOMS OF QUANTUM MECHANICS

There are three basic axioms of quantum mechanics.

- Superposition principle: It explains how a particle can be superimposed between two states at the same time.
- Measurement principle: It tells us how measuring a particle changes its state and how much information can be accessed by measurement.

- Unitary evolution: It governs how the state of the quantum system evolves over time.

Table 1. Differences between Classical and Quantum Computer

SL no	Classical computer	Quantum computer
1	Unit of information is called bit or classical bit.	Unit of information is called qubit (pronounced *cue-bit*).
2	Before and after the measurement, bit value is same, i.e. when a bit is read, the value observed is always the value stored.	The qubit after measurement is totally different from the qubit before measurement. Measurement disturbs a quantum state.
3	Bit stays in either 0 or 1 state.	Qubit can be in 0, 1 or superposition of both states.

4. BRA-KET NOTATION

A special notation, named ket notation, is used to represent quantum state. The quantum state of a particle is represented by $|\Psi>$, which is read as "ket-shai". This notation came from the physicist Paul Dirac, who wanted a concise shorthand way of writing formulas that occur in quantum physics. These formulas frequently took the form of the product of a row vector with a column vector. He referred to row vector as "bra vector" represented as $<y|$ and column vector as "ket vector" represented as $|x>$. The product of "bra" and "ket" vector is called "bra-ket" and represented as $<y|x>$ [1].

5. K-LEVEL QUANTUM SYSTEM

Let's consider a system of k distinguishable states. We can think of a Hydrogen atom. A Hydrogen atom has one electron. Let this electron be allowed to be in one of a discrete set of energy levels, starting with the ground state, the first excited state, the second excited state and so on. If we assume a suitable upper bound on the total energy, then the electron is restricted to being in one of k different energy levels – the ground state or one of k-1 excited state. Now, if we denote ground state $|0>$ and successive excited states $|1>, |2>, |3>, \tilde{}\ , |\kappa-1>$, then according to the superposition principle, the quantum state of the electron is,

$$|\Psi> = \alpha_0\, |0> + \alpha_1\, |1> + \ ...\ + \alpha_{k-1}\, |k\text{-}1> \quad (1)$$

Where $\alpha_0, \alpha_1, \alpha_2, \ldots., \alpha_{k-1}$ are complex numbers normalized so that $\sum_{j=0}^{k-1} |\alpha_j|^2 = 1$. According to Dirac's Bra-ket notation, we can write a quantum system $|\Psi>$ as a "ket" or column vector;

$$|\Psi> = \alpha_0\,|0> + \alpha_1\,|1> + \alpha_2\,|2> + \ldots + \alpha_{k\text{-}1}\,|k\text{-}1> = \begin{pmatrix} \alpha^0 \\ \alpha^1 \\ \alpha^2 \\ . \\ . \\ \alpha^{k-1} \end{pmatrix}$$

Then the "bra" of the above quantum system is the conjugate transpose of the "ket".

$$<\Psi| = (\alpha_0^* \quad \alpha_1^* \quad \alpha_2^* \quad . \quad . \quad . \quad \alpha_{k-1}^*).$$

Here, α_j* denotes the conjugate of the complex number α_j. Some example quantum states are of k=3 is,

$$|\,\Psi> = \frac{1}{\sqrt{2}}\,|0> \; + \; \frac{1}{2}\,|1> \; + \; \frac{1}{2}\,|2>,$$

$$|\,\Psi> = \frac{1+i}{3}\,|0> \; - \; \frac{1-i}{3}\,|1> \; + \frac{1+2i}{3}\,|2> \text{ etc.}$$

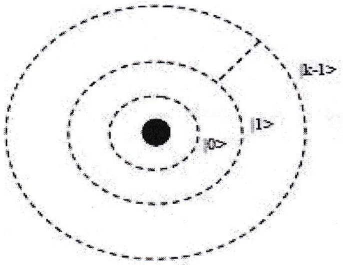

Fig. 1. The electron in Hydrogen atom can be in k different energy levels

6. HILBERT SPACE

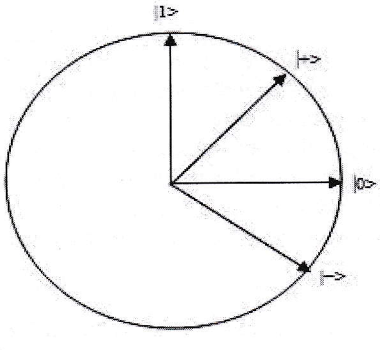

Fig. 2. Representation of qubit states in a 2-dimensional Hilbert space

If we have a k-level system, then the quantum state of the system is a point on a k-dimensional complex vector space. This complex vector space is called Hilbert space. As in the quantum state of (1) all the amplitudes α_j are normalized to 1, all the vectors in the Hilbert space are of length 1. In the Hilbert space for a quantum system, each perpendicular axes represent a basis state. From our *k*-level system, the Hilbert space consists of *k* perpendicular axes denoted by |0>, |1>, |2>, … ,|*k-1*> and the *k*-level quantum system is denoted by |Ψ>. In Hilbert space, the vector denoting the quantum state is also called "state vector". The basis states, which are represented by the perpendicular axes, are also called "Eigen states". The amplitude α_j in quantum state (1) is the projection of the state vector |Ψ> on the Eigen state vector |*j* >. An example of a 2-dimensional Hilbert space is shown in Fig. 2.

7. QUBIT

Qubit or quantum bit is the unit of quantum information. Qubit is the 2-level quantum system. For example, if we set k=2 at (1), the electron in the Hydrogen atom can be in the ground state or the first excited state, or any superposition of the two. According to the superposition principle, the quantum state of the qubit can be represented as,

$$| \Psi > = \alpha |0 > + \beta |1 >$$

$$= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Where α and β are complex numbers and $|\alpha|^2+|\beta|^2 = 1$. The state vector of the qubit is a unit vector in a 2-dimensional Hilbert space. The perpendicular axes of the Hilbert space are basis states |0> and |1>.

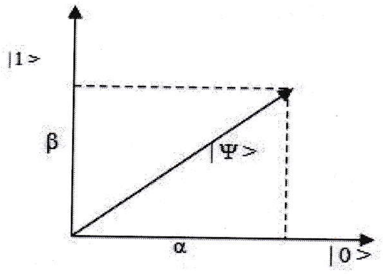

Fig. 3. A qubit |Ψ> in a 2- dimensional Hilbert Space

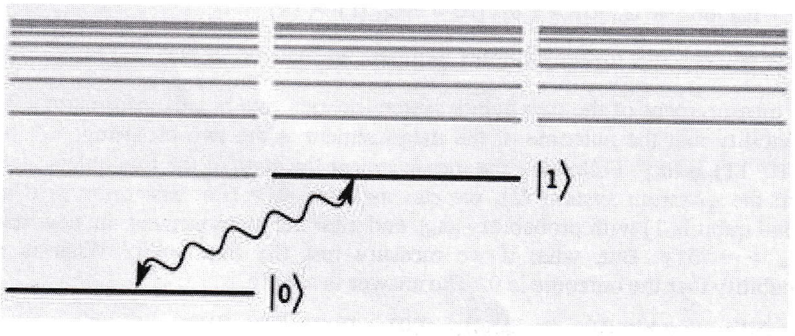

Fig. 4. Energy level diagram of an atom. Ground state and first excited state correspond to qubit levels.

According to the measurement principle, from a qubit $|\Psi> = \alpha\,|0> + \beta\,|1>$,

we can measure $|0>$ with probability $|\alpha|^2$ or, we can measure $|1>$ with probability $|\,\beta\,|^2$.

One important aspect of the measurement process is that it alters the state ($\alpha\,|0> + \beta\,|1>$) of a qubit. The effect of the measurement is that the new state is exactly the outcome of the measurement. If the outcome of the measurement of $|\Psi> = \alpha\,|0> + \beta\,|1>$ yields $|0>$, then following the measurement, the qubit is in the new state $|0>$, (i.e. no more $\alpha\,|0> + \beta\,|1>$). This implies that we can't collect any additional information about α and β by repeating the measurement. For a single qubit, it also proves the measurement axiom of quantum systems (Measurement disturbs the quantum state). Two examples of qubit are given below:

- **Atomic Orbits**

  The electrons within an atom exist in quantized energy levels. Qualitatively these electronic orbits can be thought of as resonating standing waves. Two such individual levels can be isolated to configure the basis states for a qubit [2].

- **Spins**

  The spin of a (spin-1/2) particle is a two-state system and can be described by a qubit. The spin is a quantum description of the magnetic moment of an electron which behaves like a spinning charge. The two allowed states can roughly be thought of as clockwise rotations ("spin-up") and counter clockwise rotations ("spin-down") [2].

8. ENTANGLEMENT

Let's consider a system of two qubits. We can think of two electrons in two Hydrogen atoms, each regarded as a 2-state quantum system. Since each electron can be in either of the ground state or the excited state, classically the two electrons are in one of four possible states – 00, 01, 10 and 11; and represents 2 bits of classical information. By the superposition principle, the quantum state of the two electrons can be any linear combination of these four classical states [9].

$|\Psi> = \alpha_{00}\,|00> + \alpha_{01}\,|01> + \alpha_{10}\,|10> + \alpha_{11}\,|11>$, (2)

Where α_{00}, α_{01}, α_{10}, α_{11} are complex numbers normalized so that $\Sigma_{ij}\,|\alpha_{ij}|^2 = 1$.

The measurement of the two qubits system reveals two bits of information. The probability that the outcome of the measurement is the two bit string, x ⍰ {00, 01, 10, 11} is $|\alpha_x|^2$. Following the measurement the state of the two qubits is $|x>$. From the quantum system (2), we can measure $|01>$ (i.e. first qubit is 0 and second qubit is 1) with probability $|\alpha_{01}|^2$ and after the measurement the new state, $|\Psi_{new}> = |01>$. But, what if we measure just the first qubit? What is the probability that the outcome is 0? The answer is simple.

$$\begin{aligned} \text{Probability } \{\text{1st bit: } 0\} &= \text{Probability } \{00\} + \text{Probability } \{01\} \\ &= |\alpha_{00}|^2 + |\alpha_{01}|^2 \end{aligned}$$

The new superposition is obtained by crossing out all those terms of $|\Psi>$ that are inconsistent with the outcome of the measurement (i.e. those whose first bit is 1).

$$|\Psi_{\text{new}}> = \frac{\alpha_{00}\,|00> + \alpha_{01}\,|01>}{\sqrt{|\alpha_{00}|^2 - |\alpha_{01}|^2}}$$

If the state of the first qubit is $\alpha_0|0> + \alpha_1|1>$ and the state of second qubit is $\beta_0|0> + \beta_1|1>$ then the joint state of these two qubits is $\alpha_0\,\beta_0\,|00> + \alpha_0\,\beta_1\,|01> + \alpha_1\,\beta_0\,|10> + \alpha_1\,\beta_1\,|11>$.

For example:

$$|\Psi_1> = \frac{3}{5}|0> + \frac{4}{5}|1>$$

$$|\Psi_2> = \frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>$$

$$|\Psi> = (\frac{3}{5}|0> + \frac{4}{5}|1>)\,(\frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>)$$

$$|\Psi> = \frac{3}{5\sqrt{2}}|00> - \frac{3}{5\sqrt{2}}|01> + \frac{4}{5\sqrt{2}}|10> - \frac{4}{5\sqrt{2}}|11>.$$

(3)

$$= \frac{3}{5}|0>(\frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>) + \frac{4}{5}|1>(\frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>)$$

$$= (\frac{3}{5}|0> + \frac{4}{5}|1>)(\frac{1}{\sqrt{2}}|0> - \frac{1}{\sqrt{2}}|1>)$$

An important factor about entangled state is that the entangled state can't be factored into two individual qubits. But in the last example, we can factor the composite state into two individual qubits.

Moreover, if in the quantum state (3), we measure the first qubit as 0, then the probability is,

Probability {1st bit: 0} = Probability {00} + Probability{ 01}

$$= (\frac{3}{5\sqrt{2}})^2 + (-\frac{3}{5\sqrt{2}})^2$$

$$= 0.36$$

$$\text{Then, } |\Psi_{\text{new}}> = \frac{\frac{3}{5\sqrt{2}}|00> - \frac{3}{5\sqrt{2}}|01>}{\sqrt{0.36}}$$

$$= \frac{1}{\sqrt{2}}|00> - \frac{1}{\sqrt{2}}|01>$$

Here a notable point is, after measuring first qubit, we get such a new state $|\Psi_{\text{new}}>$ where the second qubit can be still 0 or 1. It proves that the quantum state (3) is not an entangled state.

Now, let's consider another state.

$$|\Psi> = \frac{1}{\sqrt{2}}(|00> + |11>)\ (4)$$

There is no way to factor this quantum state into two individual qubits $\alpha_0|0> + \alpha_1|1>$ and $\beta_0|0> + \beta_1|1>$.

From (4), we get, $\alpha_0\ \beta_0 = \frac{1}{\sqrt{2}}$, $\alpha_0\ \beta_1 = 0$, $\alpha_1\ \beta_0 = 0$, $\alpha_1\ \beta_1 = \frac{1}{\sqrt{2}}$

As $\alpha_0\ \beta_0 = \frac{1}{\sqrt{2}}$, we are sure that $\alpha_0 \neq 0$ and $\beta_0 \neq 0$

As $\alpha_1\ \beta_1 = \frac{1}{\sqrt{2}}$, then we get, $\alpha_1 \neq 0$ and $\beta_1 \neq 0$

That means, all of the four variables are nonzero.

But $\alpha_0\ \beta_1 = 0$ and $\alpha_1\ \beta_0 = 0$ implies that some of them must be zero. For this inconsistency, it is proved that quantum state (4) can't be factored into two qubits.

Moreover, in state (4) if we measure the first qubit as 0, then

Probability {1st bit: 0} = Probability {00}

$$= (\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$$

And $|\Psi_{new} > = \dfrac{\frac{1}{\sqrt{2}}|00>}{\sqrt{\frac{1}{2}}} = |00>$

That means, when we measure first qubit as 0, the second qubit "automatically" becomes 0. Similarly if we measure first qubit as 1 (with probability 1/2), then the second qubit "automatically" becomes 1 (i.e. the new state is $|\Psi_{new}> = |11>$). This is true no matter how distant the two particles are. This interesting feature is called *entanglement*. It is a phenomenon which is responsible for much of the "quantum weirdness" that makes quantum mechanics so counter-intuitive and fascinating. From our first example of quantum system, we can say that entangled state is not just a composite state made of two qubits. We define the entangled state in the light of our second example.

"Entanglement is the composite state of two qubits where individual qubit states can not be found and the measurement of one qubit definitely affects the other one."

9. UNITARY EVOLUTION

Third axiom of quantum mechanics is unitary evolution or unitary transformation. Unitary evolution or unitary transformation is a rigid body rotation of the Hilbert space. By means of rotation of the Hilbert space, the quantum state evolves over time. A unitary transformation on a 2-dimensional Hilbert space is specified by mapping the basis states |0> and |1> to orthonormal states $|v_0> = a|0> + b|1>$ and $|v_1> = c|0> + d|1>$. It is specified by matrix,

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

If we denote $U^\dagger$ as the conjugate transpose of matrix U,

$U^{\dagger} = \begin{pmatrix} a^{*} & b^{*} \\ c^{*} & d^{*} \end{pmatrix}$,

Then it is verified as U $U^{\dagger}$ = $U^{\dagger}$U = I.

We give an example of unitary evolution.

Let, in the 0/1 basis, we have a qubit of state,

$|\Psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

If the Hilbert space is rotated 45° counterclockwise, the basis state |0> will become,

$|+\rangle = \cos 45^{\circ}\,|0\rangle + \sin 45^{\circ}\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$

And basis state |1> will become,

$|-\rangle = -\sin 45^{\circ}\,|0\rangle + \cos 45^{\circ}\,|1\rangle = -\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$

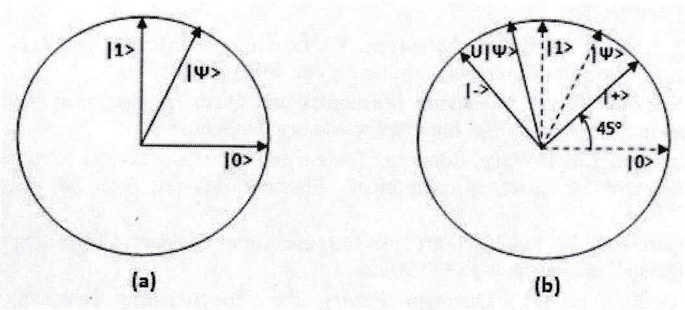

Fig. 5. (a) A qubit $|\Psi\rangle = \frac{1}{2}\,|0\rangle + \frac{\sqrt{3}}{2}\,|1\rangle$ in a 2-dimensional Hilbert space.

(b) Hilbert space rotated 45°; new qubit state U|Ψ> in +/− basis.

After rotation of the Hilbert space, the new basis states are |+> and |− >. In this +/− basis, the new state is U|Ψ>,

where $U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$

Now, $U|\Psi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{1-\sqrt{3}}{2\sqrt{2}} \\ \frac{1+\sqrt{3}}{2\sqrt{2}} \end{pmatrix}$

So, we can write, $U|\Psi\rangle = (\frac{1-\sqrt{3}}{2\sqrt{2}})\,|+\rangle + (\frac{1+\sqrt{3}}{2\sqrt{2}})\,|-\rangle$

That means, if we rotate Hilbert space, then we can measure the qubit on a new basis and vice versa.

10. CONCLUSION

After Richard Feynman surprised the world by proving that computing power can be greatly enhanced by using quantum mechanical phenomena, quantum computer has been drawing enormous interest of the mathematicians, physicists and computer scientists all over the world. For a long time, quantum computer was a theoretical computer. But in 2011, a Canadian electronics company D-wave Inc. announced the release of world's first quantum computer. Quantum computer is no more an imagination. Already some quantum algorithms like Shor's integer factorization algorithm and Grover's database search algorithm have been proved to be more efficient than the related best known classical algorithms. Now, hundreds of researches are going on in both of the fields of construction of powerful quantum computer and the development of quantum algorithms. To understand these sophisticated algorithms and to commence any type of research in quantum computing, the topics of quantum mechanics discussed in this paper must be properly realized.

11. REFERENCES

[1]. T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe and J. L. O'Brien (2010), "Quantum Computers", *Nature* , Vol. 464, pp. 45-53.

[2]. U. Vazirani (2012), "Quantum Mechanics and Quantum Computation", Lecture notes on the online course. http://www.edx.org, Unpublished.

[3]. Jialin Chen, Lingli Wang, Edoardo Charbon and Bin Wang (2013), "Programmable architecture for quantum computing", Physical Rev. A, Vol. 88, pp 022311-022324.

[4]. E. Rieffel and W. Polak (2000), "An Introduction to Quantum Computing for Non-Physicists", arXiv:quant-ph/9809016.

[5]. D. Deutsch (1985), "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer" in *Proceedings Royal Society London*, Vol. 400 no. 1818 97-117.

[6]. P. Shor (1994), "Algorithms for quantum computation: Discrete logarithms and factoring" in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Washington, DC, USA, pp. 124–134.

[7]. D. Deutsch and R. Jozsa (1992), "Rapid Solution of Problems by Quantum Computation," in *Proceedings Royal Society London*, Vol. 439A, pp. 553-558.

[8]. M. Hayward (2008), "Quantum Computing and Shor's Algorithm." Sydney: Macquarie University Mathematics Department, Unpublished.