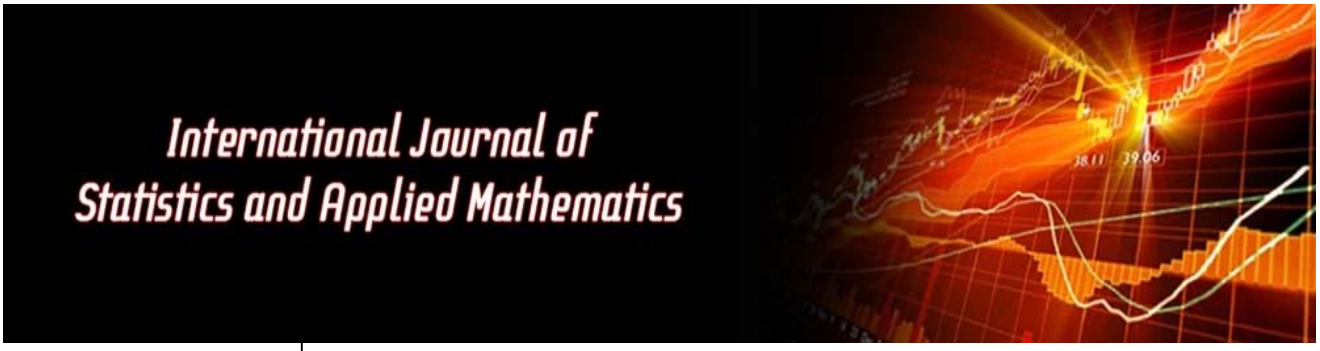
International Journal of Statistics and Applied Mathematics 2017; 2(5): 94-96



ISSN: 2456-1452
Maths 2017; 2(5): 94-96

www.mathsjournal.com
Received: 05-07-2017
Accepted: 06-08-2017

Gagandeep Aulakh
Assistant Professor, Khalsa College for Women, Sidhwan Khurd, Punjab, India

Correspondence
Gagandeep Aulakh
Assistant Professor, Khalsa College for Women, Sidhwan Khurd, Punjab, India

Introductory ideas about computation based on principles of quantum mechanics

Gagandeep Aulakh

Abstract
Basic concepts of quantum mechanics are used to build the ideas of quantum computation. Meaning of measurement in quantum physics, referring to quantum states and eigenstates is considered as the bases of quantum computation. Formation of qubits and the construction of multiple qubit system gives rise to entangled states. The Hadamard gate whose action on a set of qubits in their basis states is the first step in many quantum algorithms has also been discussed. Simple Boolean functions are used to do quantum computations which are as capable as classical computers. Difficulties to build algorithms for quantum computers are also highlighted.

Keywords: Decoherence, Eigenstates, Entangled states, Gates, Qubit

1. Introduction
In the early 1980s Richard Feynman noted that quantum systems [1] cannot be efficiently simulated on a classical computer. Till then the accepted view was that any reasonable model of computation can be efficiently simulated on a classical computer. Hence, this observation led to a lot of rethinking about the basic models of computation and the physics behind the computation. It was suggested that the dynamics of quantum systems could be used to perform computation in a much more efficient way. After this initial excitement, things slowed down for some time till 1994 when Peter Shor announced his polynomial time factorization [2] algorithm which uses quantum dynamics. The study of quantum systems for computation has come into its own since then.

2. Quantum Physics Basics
Consider an electron (say, in an Hydrogen atom) with two energy levels (ground state and one excited state). In general, the electron can be in a superposition of both the states. We represent these two 'basis' states by |0> and |1> where | > is called a 'ket' (this notation, introduced by Dirac, the 'bra' < | and the 'ket' | >). The ket is just a convenient representation for a column vector. For the above system such a vector space could be any two dimensional complex vector space. Any state of the electron can thus be represented as a |0> + b |1>. The inner product of two vectors |x> and |y> is written as the bra-ket combination <x||y>. The outer product |x>< y | of two vectors x and y is a linear transformation operator, which is equivalent to the matrix $xy^{T.}$ Now that we have this notation, we will state a very basic fact about quantum states: as soon as one makes a measurement on an unknown quantum state, it collapses to one of the eigenstates, each measurement having a specific set of eigenstates. For example, in case of electron once we make a measurement the quantum state continues to be in the state measured. Thus, a|0> + b|1> → measure → |0> or |1>.

3. Qubits
The simplest quantum state |a> + |b> is called a qubit, or a quantum bit. The qubit [3] could represent any 2 dimensional quantum vectors, such as the state of an electron in an atom with just two energy levels. The qubit is normalized such that $|a|^2 + |b|^2 = 1$, so that $|a|^2$ and $|b|^2$ represent the probabilities. Once measured, the qubit continues to remain in the state measured.

4. Multiple Qubit Systems

When quantum systems combine, the resultant state space of the combined system is obtained by the tensor product [4] of the state spaces of the combining systems. Let us first examine the differences between the tensor product and cartesian product. If spaces with dimensions m and *n,* respectively, combine through the Cartesian product, the resultant space has dimensions *m+n,* whereas if they combine through the tensor product the resultant space has a dimension of *mn.* The possibility of linear superposition with tensor product provides a very interesting feature of quantum systems - the ability to interpret the action of separate Gates [5] on separate spaces as an operator on the combined space.

5. Entangled States

The states, which cannot be split into separate qubits are called entangled[6] states. They cannot be specified by specifying the states of the constituent qubits. These kind of systems have no analogue in the macroscopic world where the description of any system can be broken down into that of its parts. Thus, entangled states defy classical thinking. There are other states where a measurement of one qubit does not completely determine the other one, but changes its probabilities of measurement. Therefore, entangled states can also be defined to be those states in which the measurement of one qubit affects the results of measurements of other qubits. Consider a XOR gate acting on two classical bits as shown in Figure 1. Here, an arbitrary bit can be duplicated. But such is not the case with qubits. There exists no unitary transformation *U* that can duplicate arbitrary qubits.

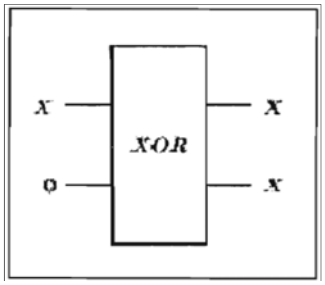


Fig 1

6. Measurement

A measurement of a quantum system is a disturbance of the system such that the system collapses to one of a set of eigenstates. Thus, every measurement of a quantum system has associated eigenstates. What is important to understand is that once measured the qubit continues to remain in that state, i.e. it continues to give the same measured value, if further measurements are made with respect to the same eigenstates. In a multiple qubit system measurements of one or more qubits collapses the system to a superposition compatible with the measured values.

7. Qubit Dynamics

We will represent the transformation of qubits, i.e. the transformations of quantum systems from one state to another as actions of quantum gates. This dynamics is governed by the Schrodinger equation, which implies that the inner product of the underlying space is preserved during any transition between states (i.e., orthogonality is preserved). Linear transformations which preserve orthogonality are called unitary transformations[7] and have the special property that $UU^* = I$ (where U^* is called the adjoint, in a matrix representation, the adjoint is the complex conjugate of the transpose matrix). From this property we can easily see that a unitary transformation will be reversible, the inverse transformation being U^*. We will be representing a gate by specifying the action it performs on the basis states; action on arbitrary qubits can be derived using linearity.

8. Single Qubit Gates

Other than identity, the only classical single bit gate is the NOT gate (which flips the state). The quantum analogue of this can be imagined as a 180 degree rotation about the *y* axis on the qubit sphere [8]. However, rotation by all other angles is also possible, yielding a variety of other gates. Some of these are

1. The Identity transformation,
   I: $|0> \rightarrow |0>$ and $|1> \rightarrow |1>$
2. Negation,
   X: $|0> \rightarrow |1>$ and $|1> \rightarrow |0>$
3. Phase Shift,
   Z: $|0> \rightarrow |0>$ and $|1> \rightarrow -|1>$
4. A combination of negation and phase shift,
   Y: $|0> \rightarrow -|1>$ and $|1> \rightarrow |0>$
5. The Walsh–Hadamard transformation,
   H: $|0> \rightarrow \frac{1}{\sqrt{2}}(|0> + |1>$
   $|1> \rightarrow \frac{1}{\sqrt{2}}(|0> - |1>)$

Note particularly the last one of the above transformations, known as the Hadamard gate [9]. It takes in a qubit in one of the basis states and puts it into a superposition. The action by this gate on a set of qubits in their basis states is the first step in many quantum algorithms.

9. Multi Bit Gates and the Quantum Computer

We know that all the classical circuits can be synthesized using only the AND and NOT gates. The classical NOT gate is a reversible gate (being its own inverse). We have an analogous quantum NOT gate. However, we notice that the classical AND gate is a non-reversible gate. So we circumvent the problem by reproducing the inputs at the output, along with the ANDed output. This can be done by using the 3-bit controlled-controlled (or the Toffoli) gate [10, 11] which flips the third input if the first two are both |1>.

The most important two bit gate is the C_{NOT} (controlled NOT) gate which acts on two qubits, flipping the second qubit (controlled qubit) if the first qubit (controlling qubit) is |1> and otherwise leaving the second qubit unchanged. Using the outer product notation shown in the section on qubits, we can write the Toffoli gate's action as

$$T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{\mathrm{NOT}}$$

where the C_{NOT} itself can be broken into simpler gates as

$$C_{\mathrm{NOT}} = |0\rangle\langle 0| \otimes I + |1\rangle|1\rangle \otimes X.$$

Thus, we have

$$T = |0\rangle\langle 0| \otimes I \otimes I + (|1\rangle\langle 1|) \otimes (|0\rangle\langle 0|) \otimes I +$$
$$(|1\rangle\langle 1|) \otimes (|1\rangle\langle 1|) \otimes X.$$

Here |0> <0| is the transform that takes |0> to |0> and |1> to $(O,O)^T$

So the first term in the expression for *T* acts on the first bit by changing it to the scalar 0 if it is |1> and leaving it unchanged if it is |0>. The second and third bits are left unaffected. The net result is that the first term leaves the three qubit set unchanged if the first qubit is |0> and changes it to the scalar 0 if the first bit is |1>. The other two terms can be understood similarly. As an example, consider the action of the Toffoli gate on |110>. The first and the second terms in the expression give the scalar 0 as output. The third term gives |111>. The overall result, as you can deduce, is

$$T|110\rangle \rightarrow |111\rangle,$$

which fits in with our earlier description of the gate. We can construct a reversible AND gate by acting with the Toffoli gate on |x,y,0>.

$$T|x,y,0\rangle \rightarrow |x,y,x\text{AND}y\rangle$$

Having reversible AND and NOT gates in our possession, we can realize any Boolean function by using arrays of these gates [12, 13, 14] (i.e., a quantum computer, capable of performing any task a classical computer can perform, can be built).

10. Conclusion

The principles of quantum physics can be exploited in making a computational device. However, we still haven't seen the kind of algorithms a quantum computer would use and how they would be different from traditional algorithms. Currently, apart from a very few algorithms, not much is known about the programming of such computers. The fundamental obstacle to building a quantum computer is that of decoherence. The interaction of a quantum system with the environment obstructs the unitary evolution of the system and causes dissipation of information, reducing coherence of information. In simpler words, the interaction with the environment is like making a measurement before the computation has been completed. It has been shown that decoherence can't be efficiently removed by simply repeating the computation many times. Technologists are working to reduce the effects of decoherence by employing techniques that allow more computation steps before the time when the effects of decoherence become significant. A lot of work needs to be done not only on the physical side, but also on the algorithmic side, if we are to make the promises of this technology come true.

11. References

1. Shor P. Proceedings of the 37th Symposium on the Foundations of Computer Science, 1996, 56.
2. Aharonov D, Ben-Or M. arXiv quant-ph/9611025, 1996.
3. Knill E, Laflamme R, Zurek W. Phys. Rev. B. 1998; 453:365.
4. Read N, Green D. Phys. Rev. B. 2000; 61:10267.
5. Levin MA, Wen XG. Phys. Rev. B 2005; 71:045110.
6. Kauffman LH. Knots and Physics, 1993.
7. Wilczek F. Phys. Rev. Lett. 1982; 48:1144.
8. Wilczek F. Phys. Rev. Lett. 1982; 48:1146.
9. Sakurai JJ. Modern Quantum Mechanics, 1993.
10. Kitaev A, Annals of Physics. 2003; 303:2.
11. Stern A. Annals of Physics. 2008; 323:204.
12. Nayak C, Simon SH, Stern A, Freedman M, Das Sarma S. Rev. Mod. Phys. 2008; 80:1083.
13. Alicea J, Rep. Prog Phys. 2012; 75:076501.
14. Leijnse M, Flensberg K. Semicond. Sci. Technol. 2012; 27:124003.
15. Hassler F. arXiv quant-ph/1404, 2014, 0897.
16. Burnell FJ, Nayak C. Phys. Rev. B. 2011; 84:125125.