Glimpses of Quantum Computation

Samir Roy*

Abstract

Quantum computation is a promising field of study because the conventional computer hardware is fast reaching its limit of computational power. A further advancement can be achieved only by a completely different set of physical properties and operations. This paper presents a brief overview of the fundamental concepts of quantum computation. The concept of a quantum bit, in contrast with the classical bit, is explained. The quantum logic gates and quantum circuits are described along with appropiate examples. Quantum parallelism, a phenomenon that is at the root of the power of quantum computation, is explained briefly.

Keywords - Quantum mechanics, Qubit, Controlled logic, Teleportation, EPR pair

1. Introduction

Manin [1] pointed out that computers built upon the principles of quantum mechanics might simulate quantum systems more efficiently than classical computers. Subsequently, this was echoed by Richard Feynmann in 1982 when he observed that it is difficult to simulate quantum phenomena on classical computers. He suggested that computers that work on the principles of quantum mechanics should be more suitable to do the job. The study of quantum computation, as a purely intellectual activity, has started by then. A quantum Turing Machine (TM) was introduced in 1980 [2]. In 1985, Deutsch [3] presented the notion of a universal quantum computer. Benette and Weisner invented superdanse coding [4] in 1992. In superdanse coding, two classical bits can be transmitted using only one bit. It is based on the strange quantum mechanical properties of Einstein-Podolsky-Rosen (EPR) pair [5]. Quantum teleportation, a technique for moving quantum states around even in absence of quantum communication channel linking the sender of the quantum state to the recipient, was proposed by Bennett et al [6] in 1993. The most spectacular success in the field of quantum computing came in 1994, with Shor's famous quantum algorithm for prime factorization [7, 8]. Finding prime factors of large integers is a complex problem. Many encryption algorithms use this complexity as the basis for building security systems for computers. Shor's polynomial time alogorithm for prime factorization has jeopardized all these encryption systems. In 1996, superdanse coding was experimentally verified [9]. Teleportation too has been implemented in various ways [10, 11, 12, 13].

Quantum computers are now a reality. Issac Chuang of IBM has reported in December 2001, a 7-qubit quantum computers that implemented Shor's factorizing algorithm to factorize 15 (=3'5). Intensive research is going on worldwide to build quantum computers that can solve practical problems. With VLSI technology fast approaching its saturation point, it is almost certain that the future of computation lies in the paradigm of quantum computing.

Rest of the paper is organized as follows. *Section 2* introduces the concept of a quantum bit, popularly known as qubit, that forms the basis of quantum computation. Fundamentals of quantum computation are presented in *Section 3*. *Section 4* points out the hidden power of quantum computation that is yet to be harnessed to get useful work. Conclusions are drawn in *Section 5*.

*Lecturer, Computer Science & Engineering

2. The Quantum Bit (Qubit)

A classical bit has two states , *viz.*, 0 and 1. At any instant, it is either in the 0 state or in the 1 state. A quantum bit, referred to as *qubit*, has infinitely many states among which the states $|0\rangle$ anf $|1\rangle$ are two orthogonal states. $|0\rangle$ ($|1\rangle$) is the notation for state 0 (1) in the context of quantum computation. An arbitary state $|\Psi\rangle$ of a qubit is a linear combination or superposition of the orthogonal basis $|0\rangle$ and $|1\rangle$:

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

Where α and β are complex numbers, though quite often real numbers also.

The most interesting characteristic of a qubit is, we cannot measure a qubit in its quantum state $|\Psi\rangle$. The fact is as soon as we measure a qubit , its state collapses to $|0\rangle$ or $|1\rangle$ either with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively. Obviously $|\alpha|^2 + |\beta|^2 = 1$

Now, consider a closed system consisting of two qubits. Classicaly, there are four possible configurations, *viz* 00, 01, 10 and 11, for a pair of bits. The quantum equivalent of these states, represented as $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ respectively, form the orthogonal basis for the quantum state of this qubit system.

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

On measurement, $|\Psi\rangle$ will produce the states $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$ with probabilities $|\alpha_{00}|^2$ $|\alpha_{01}|^2$, $|\alpha_{10}|^2$, and $|\alpha_{11}|^2$ respectively. The complex coefficients α_{00}, α_{01}, α_{10} and α_{11} must satisfy the following normalization condition

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1 \quad (3)$$

For a system of n qubits, the computational basis consists of the orthogonal states $|x_1 x_2 x_3 \ldots x_n\rangle$, $x_i \in \{0,1\}$. The quantum states of such a system are specified by 2^n number of probability amplitudes. This opens up the possibility of tremendous computational power provided we knew how to harness that power.

3. Quantum Computation

Just as a classical computer is built with electronic circuits that consist of logic gates and interconnections among them, a quantum computer is also built with *quantum circuits*. A quantum circuit is built upon elementary *quantum gates* and *quantum wires*. The following subsections describe these aspects very briefly.

3.1 Single Quantum Gates

The only non-trivial classical single bit gate is the NOT gate that performs the mapping $0\rightarrow1$ and $1\rightarrow0$. How to extend this idea to a quantum NOT gate that operates on a single qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$? Such a gate should perform the transformation $|\Psi\rangle\rightarrow|\Psi'\rangle$ where $|\Psi'\rangle = \beta|0\rangle + \alpha|1\rangle$. Thus, the effect of the quantum NOT on $|\Psi\rangle$ is a reversal of the probabilities with which $|\Psi\rangle$ collapses to $|0\rangle$ or $|1\rangle$ on measurement.

A quantum NOT gate can be conveniently expressed as a unitary matrix X (in quantum computation, NOT is expressed with X for historical reason). In fact, it is one of the fundamental postulates of quantum mechanics that every operation performed on a quantum state can be represented by a unitary matrix. Therefore, in vector notation, a quantum NOT operation is described as follows :

$$X\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

Where

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

Apart from quantum NOT, there are other interesting single qubit gates. Among these, two important single qubit gates are the Zgate and the Hgate, as defined below.

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

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

H is also known as the *Handamard* gate and is extremely useful in quantum computation. It is also described as the "square root of NOT gate". The Hadamard gate turns |0> onto (|0>+|1>)/ √2 which is halfway between |0> and |1>. The schematic diagrams of the qubit gates *X*, *Z* and *H* are shown in *Fig 1.*

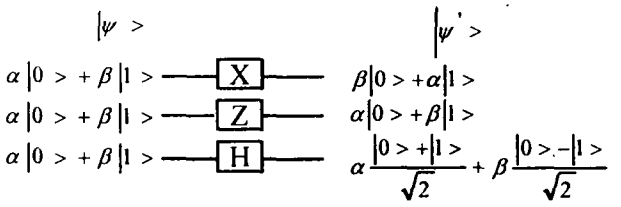


Fig. 1 : Single qubit logic gates

3.2 Multiple Qubit Logic Gates

The controlled-NOT, or CNOT, is the protopype multiple qubit logic gate. The logic diagram and the transformation matrix for CNOT are shown in *Fig. 2.*

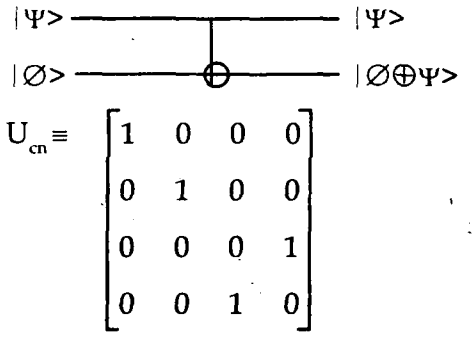


Fig. 2 : The CNOT quantum logic gate

The action of a CNOT is summarised in the following transformtions :

|00> → |00>, |01>→ |01>, |10>→ |11>, |11>→|10>

In the other words, it passes one of its inputs, the control bit, unaltered and flips the other bit only if the control bit is 1.

3.3 Quantum Circuits

To have a taste of what constitutes a quantum circuit, let us consider the simple operation of swapping the states of two qubits, *i.e.* the transformation $|a,b\rangle \rightarrow |b,a\rangle$. The logic diagram of a quantum circuit to carry out this task is shown in *Fig. 3.*

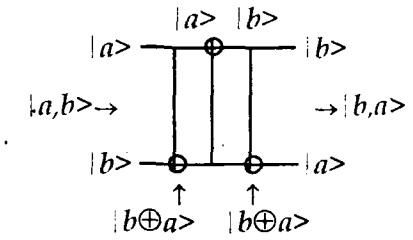


Fig. 3 : A quantum circuit to perform $|a, b\rangle \rightarrow |b,a\rangle$

The circuit accomplishes the following sequence of transformations :

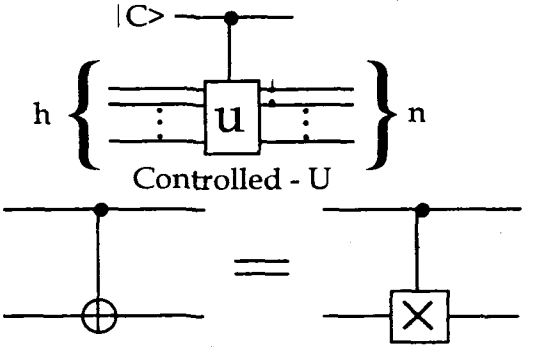
$$|a,b\rangle \rightarrow |a, a\oplus b\rangle$$

$$\rightarrow |a\oplus(a\oplus b), a\oplus b\rangle = |b,a\oplus b\rangle$$

$$\rightarrow |b, (a\oplus b)\oplus b\rangle = |b, a\rangle$$

The lines in *Fig. 3* represent quantum wires that transfer quantum information through space and/or time. It may not be a physical wire. It may, perhaps, be simply a passage of time, or perhaps a photon moving through space.

While drawing a quantum circuit it is customary to represent controlled-*U* operation, where *U* is a unitary matrix, as shown in *Fig. 4*. Here *U* is an *n* bit logic operation. The logic symbol for a quantum measurement is shown in *Fig. 5.*



Two different representations of controlled -NOT

Fig. 4 : Conventions of drawing controlled logic operation in quantum computation

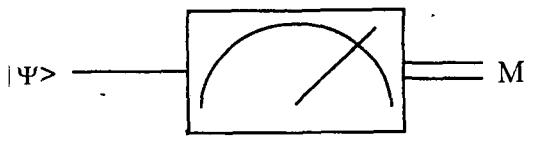


Fig. 5 : Circuit symbol for quantum measurement

Take for example the case of an *Einstein-Podolsky-Rosen* (*EPR*) pair of entangled bits. Consider the quantum circuit of *Fig. 6* that consists of a Handamard gate followed by a CNOT.

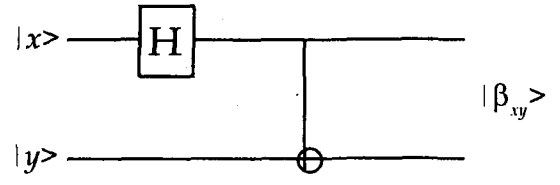


Fig. 6 : Quantum circuit manipulating an EPR pair

Suppose the input state $|xy\rangle$ is $|00\rangle$. The Hadamard gate on the first bit transforms the state $|00\rangle$ to $(|0\rangle+|1\rangle)\,|1\rangle/\sqrt{2}$. Then the CNOT gives the output state $(|00\rangle+|11\rangle)/\sqrt{2}$. The output states corresponding to the input states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are given in *Table 1*.

Table - 1

In	Out
$\|00\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle+\|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle+\|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

These output states $|\beta_{00}\rangle$, $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ and $|\beta_{11}\rangle$ are known as the *Bell* states, or *EPR* pairs. *EPR* pairs have strange quantum mechanical properties.

4. Quantum Parallelism : The Power of Quantum Computation

The power of quantum computation rests on the fact that it opens up a possibility of evaluatiing a function $f(x)$ for all possible values of x simultaneously. This is known as quantum parallelism. This section briefly explains the idea of quantum parallelism.

Let us consider a function $f(x) : \{0,1\} \rightarrow \{0,1\}$. In order to carry out the computation of $f(x)$, it is possible to start with a pair $|x,y\rangle$ of qubits and, with an appropriate sequence of logic gates, transform $|x,y\rangle$ to $|x,y\oplus f(x)\rangle$. Let u_f be the total transformation $|x,y\rangle \rightarrow |x,y\oplus f(x)\rangle$. The schematic diagram of u_f is shown in Fig. 7.

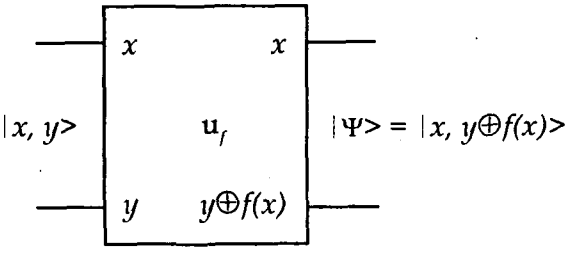


Fig. 7 : schematic diagram of u_f : $|x, y\rangle \rightarrow |x, y\oplus f(x)\rangle$

Now, consider the circuit shown in *Fig. 8* where instead of $|0\rangle$ or $|1\rangle$, $(|0\rangle+|1\rangle)/\sqrt{2}$ is applied at x. We can easily obtain $(|0\rangle+|1\rangle)/\sqrt{2}$ from a $|0\rangle$ using a Hadamard transformation. When we apply u_f, we obtain the following state

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{2}$$

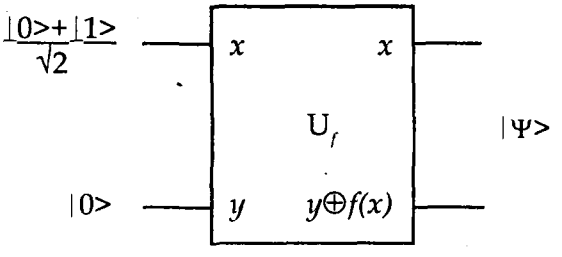


Fig. 8

The state $(|0,f(0)\rangle+|1,f(1)\rangle/\sqrt{2}$ is an extremely significant state because it contains information for $f(0)$ as well as $f(1)$. Moreover, the

evaluation of $f(0)$ and $f(1)$ are carried out absolutely simultaneously and using the same precessing unit! This is known as quantum parallelism. The above phenomenon is true for n bits also. if $f(x)$ is an n bit function, then performing u_f on

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x>$$

we compute $f(x)$ for 2^n values of x simultaneously.

5. Conclusions

The fundamental concepts of quatum computation have been presented in this paper. The concept of a quantum bit, in contrast with the classical bit, is explained. The idea of quantum logic gates as well as quantum circuits are described along with appropriate examples. Quantum parallelism, a phenomenon that is at the root of the power of quantum computation, is explained briefly. Quantum computation is a promising field of study because the conventional computer hardware is fast reaching its limit of computtional power. A further advancement can be achieved only by a completely different set of physical properties and operations. Consequently, quantum computation is fast growing as an alternative computational paradigm.

References

1. Y Manin, Computable and Uncomputable. Sovetskoye Radio, Mascow, 1980.

2. P Benioff, The computer as a physical system : A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, J. of Statistical Physics, 22(5):563-591, 1980.

3. D Deutsch, Quantum Theory, the Church-Turing Principle and the universal quantum computer. Proc. R. Soc. Lond. A, 400:97, 1985.

4. C H Bennett and S J Weisner. Communication via one-and two particle operators on Einstein-Podolsky-Rosen States. Phys. Rev. Lett., 69(20):2881-2884, 1992.

5. A Einstein, B Podolsky and N Rosen, Can quantum mechanical description of physical reality be considered complete? Phys. Rev., 47:777-780, 1935.

6. C H Bennett, G Brassard, C Crepeau, R Jozsa, A Peres and W Wootters, Teleporting an unknown quantum state via dual classical and EPR chanels. Phys. Rev. Lett., 70:1895-1899, 1993.

7. PW Shor, Algorthms for quantum computation : discrete logarithms and factoring. In Proc. of 35th Aual Symposium of Foundations of Computer Science, IEEE Press, Los Alamitos, CA, 1994.

8. P W Shor, Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comp., 26(5) : 1484-1509, 1997.

9. K Mattle, H Weinfurther, P G. Kwiat and A Zeilinger. Dense coding in experimental quantum communication. Phys. Rev. Lett., 76(25) : 4656-4659, 1996.

10. D Boschi, S Branca, F D Martini, L Hardy and S Popescu, Emperimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podylsky-Rosen channels. Phys. Rev. Lett., 80:1121-1125, 1998.

11. D Bouwmeester, J W Pan, K Mattle, M Eibl, H Weinfurther and A Zeilinger, Experimental quantum teleportation. Nature, 390(6660) : 575-579, 1997.

12. A Furusawa, J L Sorensen, S L Braunstein, C A Fuchs, H J Kimble and E S Polzik, Unconditional quantum teleportation. Science, 282:706-709, 1998.

13. M A Nielsen, E Knill and R Laflamme, Complete quantum teleportation using nuclear magnetic resonance. Nature, 396(6706):52-55, 1998.