Quantum Computing: An Introduction

Megha Khandelwal and Subho Sankar Chatterjee

[1]meghaworld29@gmail.com

[2]subhochatterjee21@yahoo.com

Abstract— Quantum computing is a subject that assembles ideas from classical quantum physics, information theory, and computer science. This paper describes the connection between information theory and quantum mechanics. Explaining their relationship, the review concocts introduction to classical information theory and computer science, including Shannon's theorem, error correcting codes, Turing machines and computational complexity. The principles of quantum mechanics are then outlined, and the EPR experiment described. The EPR-Bell correlations and quantum entanglement in general, form the essential new ingredient which distinguishes quantum from classical information theory, and arguably, quantum from classical physics. Basic Quantum information ideas are described, including key distribution, teleportation, data compression, quantum error correction, the universal quantum computer and quantum algorithms. The common theme of all these ideas is the use of quantum entanglement as a computational resource. Experimental methods for small quantum processors are briefly sketched, concentrating on ion traps, high Q cavities, and NMR. The review concludes with an outline of the main features of quantum information physics, and avenues for future research.

Index Terms— Qubits, Quantum gates, Bloch sphere, Quantum Algorithms, Quantum circuits, Quantum communication.

1 INTRODUCTION

Quantum computing was first proposed in the 1970s, it relies on quantum physics by taking advantage of certain quantum physics properties of atoms or nuclei that allow them to work together as quantum bits, or qubits, to be the computer's processor and memory. By interacting with each other while being isolated from the external environment, qubits can perform certain calculations exponentially faster than conventional computers.

Qubits do not rely on the traditional binary nature of computing. While traditional computers encode information into bits using binary numbers, either a 0 or 1, and can only do calculations on one set of numbers at once, quantum computers encode information as a series of quantum-mechanical states such as spin directions of electrons or polarization orientations of a photon that might represent a 1 or a 0, might represent a combination of the two or might represent a number expressing that the state of the qubit is somewhere between 1 and 0, or a superposition of many different numbers at once. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously, which a binary system cannot do, and also has some ability to produce interference between various different numbers. By doing a computation on many different numbers at once and, then interfering the results to get a single answer, a quantum computer has the potential to be much more powerful than a classical computer of the same size. In using only a single processing unit, a quantum computer can naturally perform myriad operations in parallel.

2 BASICS

In this section we will review the basic paradigm for quantum algorithms, namely the quantum circuit model, which is composed of the basic quantum units of information (qubits) and the basic logical manipulations thereof (quantum gates).

2.1 The Qubits

The qubit is the quantum analogue of the bit, the classical fundamental unit of information. It is a mathematical object with specific properties that can be realized physically in many different ways as an actual physical system. Just as the classical bit has a state (either 0 or 1), a qubit also has a state. Yet contrary to the classical bit, $|0\rangle$ and $|1\rangle$ are but two possible states of the qubit, and any linear combination (superposition) thereof is also physically possible. In general, thus, the physical state of a qubit is the superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (where α and β are complex numbers). The state of a qubit can be described as a vector in a two-dimensional Hilbert space, a complex vector space entry on The special states $|0\rangle$ and $|1\rangle$ are known as the computational basis states, and form an orthonormal basis for this vector space. According to quantum theory, when we try to measure the qubit in this basis in order to determine its state, we get either $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. Since $|\alpha|^2 + |\beta|^2 = 1$ (i.e., the qubit is a unit vector in the aforementioned two-dimensional Hilbert state), we may (ignoring the overall phase factor)

effectively write its state as $|\psi\rangle = \cos(\theta)|0\rangle + e^{i\phi}\sin(\theta)|1\rangle$, where the numbers θ and ϕ define a point on the unit three-dimensional sphere, as shown here. This sphere is often called the Bloch sphere, and it provides a useful means to visualize the state of a single qubit.

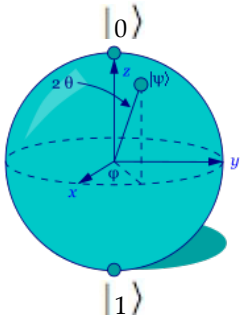

Fig1. Bloch sphere

The Bloch Sphere

Theoretically, a single qubit can store an infinite amount of information, yet when measured it yields only the classical result (0 or 1) with certain probabilities that are specified by the quantum state. In other words, the measurement changes the state of the qubit, collapsing it from the superposition to one of its terms. The crucial point is that unless the qubit is measured, the amount of hidden information it stores is conserved under the dynamic evolution (namely, Schrödinger's equation). This feature of quantum mechanics allows one to manipulate the information stored in unmeasured qubits with quantum gates, and is one of the sources for the putative power of quantum computers.

To see why, let us suppose we have two qubits at our disposal. If these were classical bits, then they could be in four possible states (00, 01, 10, and 11). Correspondingly, a pair of qubits has four computational basis states ($|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$). But while a single classical two-bit register can store these numbers only one at a time, a pair of qubits can also exist in a superposition of these four basis states, each of which with its own complex coefficient (whose mod square, being interpreted as probability, is normalized). As long as the quantum system evolves unitarily and is unmeasured, all four possible states are simultaneously "stored" in a single two-qubit quantum register. More generally, the amount of information that can be stored in a system of n unmeasured qubits grows exponentially in n. The difficult task, however, is to retrieve this information efficiently

2.2 Quantum Gates

Classical computational gates are Boolean logic gates that perform manipulations of the information stored in the bits. In quantum computing these gates are represented by matrices, and can be visualized as rotations of the quantum state on the Bloch sphere. This visualization represents the fact that quantum gates are unitary operators, i.e., they preserve the norm of the quantum state (if U is a matrix describing a single qubit gate, then $U^{\dagger}U=I$, where $U^{\dagger}$ is the adjoint of *U*, obtained by transposing and then complex-conjugating U). As in the case of classical computing, where there exists a universal gate (the combinations of which can be used to compute any computable function), namely, the NAND gate which results from performing an AND gate and then a NOT gate, in quantum computing it was shown (Barenco et al., 1995) that any multiple qubit logic gate may be composed from a quantum CNOT gate (which operates on a multiple qubit by flipping or preserving the target bit given the state of the control bit, an operation analogous to the classical XOR, i.e., the exclusive OR gate) and single qubit gates. One feature of quantum gates that distinguishes them from classical gates is that they are reversible: the inverse of a unitary matrix is also a unitary matrix, and thus a quantum gate can always be inverted by another quantum gate.

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

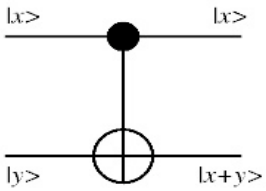

Fig2. Quantum gates

The CNOT Gate

Unitary gates manipulate the information stored in the quantum register, and in this sense ordinary (unitary) quantum evolution can be regarded as computation. In order to read the result of this computation, however, the quantum register must be measured. The measurement gate is a non-unitary gate that "collapses" the quantum superposition in the register onto one of its terms with the corresponding probability. Usually this measurement is done in the computational basis, but since quantum mechanics allows one to express an arbitrary state as a linear combination of

basis states, provided that the states are orthonormal (a condition that ensures normalization) one can in principle measure the register in any arbitrary orthonormal basis. This, however, doesn't mean that measurements in different bases are efficiently equivalent. Indeed, one of the difficulties in constructing efficient quantum algorithms stems exactly from the fact that measurement collapses the state, and some measurements are much more complicated than others.

2.3 Quantum Circuits

Quantum circuits are similar to classical computer circuits in that they consist of wires and logical gates. The wires are used to carry the information, while the gates manipulate it (note that the wires do not correspond to physical wires; they may correspond to a physical particle, a photon, moving from one location to another in space, or even to time-evolution). Conventionally, the input of the quantum circuit is assumed to be a computational basis state, usually the state consisting of all $|0\rangle$. The output state of the circuit is then measured in the computational basis, or in any other arbitrary orthonormal basis. The first quantum algorithms (i.e. Deutsch-Jozsa, Simon, Shor and Grover) were constructed in this paradigm. Additional paradigms for quantum computing exist today that differ from the quantum circuit model in many interesting ways. So far, however, they all have been demonstrated to be computationally equivalent to the circuit model (see below), in the sense that any computational problem that can be solved by the circuit model can be solved by these new models with only a polynomial overhead in computational resources.

3 QUANTUM ALGORITHM

The power of quantum computing could only be harnessed an algorithm could exploit the potential of it. An algorithm is simply a program that is designed for the purpose of solving a certain problem. Without algorithms, we would have no computer (classical or quantum), because there would have been no motivation to build a computer if it could not solve any problems.

3.1 Shor's Algorithm

Shor's algorithm, named after mathematician Peter Shor, is a quantum algorithm (an algorithm which runs on a quantum computer) for integer factorization discovered in 1994. Informally it solves the following problem: Given an integer N, find its prime factors.

On a quantum computer, to factor an integer N, Shor's algorithm runs in polynomial time (the time taken is polynomial in log N, which is the size of the input[1]). Specifically it takes time $O((\log N)^3)$, demonstrating that the integer factorization problem can be efficiently solved on a quantum computer and is thus in the complexity class BQP. This is exponentially faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time -- about $O(e^{(\log N)1/3 (\log \log N)2/3})$. The efficiency lies in the efficiency of the quantum Fourier transform, and modular exponentiation by squarings.

Shor's algorithm is important because it can, using a quantum computer, be used to break the widely used public-key cryptography scheme known as RSA. RSA is based on the assumption that factoring large numbers is computationally infeasible. So far as is known, this assumption is valid for classical (non-quantum) computers; no classical algorithm is known that can factor in polynomial time. However, Shor's algorithm shows that factoring is efficient on a quantum computer, so an appropriately large quantum computer can break RSA. It was also a powerful motivator for the design and construction of quantum computers and for the study of new quantum computer algorithms. It has also facilitated research on new cryptosystems that are secure from quantum computers, collectively called post-quantum cryptography.

In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3 × 5, using an NMR implementation of a quantum computer with 7 qubits.[2] However, some doubts have been raised as to whether IBM's experiment was a true demonstration of quantum computation, since no entanglement was observed.[3] Since IBM's implementation, several other groups have implemented Shor's algorithm using photonic qubits, emphasizing that entanglement was observed.

3.2 Grover's Algorithm

Suppose you have met someone who kept her name secret, but revealed her telephone number to you. Can you find out her name using her number and a phone directory? In the worst case, if there are n entries in the directory, the computational resources required will be linear in n. Grover showed how this task, namely, searching an unstructured database, could be done with a quantum algorithm with complexity of the order √n. Agreed, this "speed-up" is more modest than Shor's since searching an unstructured database belongs to the class **P**, but contrary to Shor's case, where the classical complexity of factoring is still unknown, here the superiority of the quantum algorithm, however modest, is definitely provable. That this quadratic "speed-up" is also the optimal quantum "speed-up" possible for this problem was proved by Bennett, Bernstein, Brassard and Vazirani.

Although the purpose of Grover's algorithm is usually described as "searching a database", it may be more accurate to describe it as "inverting a function". Roughly speaking, if we have a function y=f(x) that can be evaluated on a

quantum computer, Grover's algorithm allows us to calculate *x* when given *y*. Inverting a function is related to searching a database because we could come up with a function that produces a particular value of *y* if *x* matches a desired entry in a database, and another value of y for other values of x. The applications of this algorithm are far-reaching (over and above finding the name of the mystery 'date' above). For example, it can be used to determine efficiently the number of solutions to an *N*-item search problem, hence to perform exhaustive searches on a class of solutions to an NP-complete problem and substantially reduce the computational resources required for solving it.

4 CRYPTOGRAPHY AND ENCRYPTION

In the age where buying, banking and almost anything can be done online; security and encryption is imperative. RSA is the most secure encryption that is used today, because even the most advanced supercomputers cannot crack the system. Why? Because in order to break the RSA encryption, it is reduced to factoring extremely large numbers (300 digit integers), which even the fastest computers and supercomputers today choke when attempting. In fact it would take hundreds of years to find the factors of a 300 digit integer using the fastest supercomputer, yet by using Shor's Algorithm on a quantum.

5 CHALLENGES

The current challenge is not to build a full quantum computer right away but rather to move from the experiments in which we merely observe quantum phenomena to experiments in which we can control these phenomena. This is a first step towards quantum logic gates and simple quantum networks.

Experimental and theoretical research in quantum computation is accelerating worldwide. New technologies for realizing quantum computers are being proposed, and new types of quantum computation with various advantages over classical computation are continually being discovered and analyzed and we believe some of them will bear technological fruit. From a fundamental standpoint, however, it does not matter how useful quantum computation turns out to be, nor does it matter whether we build the first quantum computer tomorrow, next year or centuries from now. The quantum theory of computation must in any case be an integral part of the worldview of anyone who seeks a fundamental understanding of the quantum theory and the processing of information.

6 ADVANTAGES

There are several reasons that researchers are working so hard to develop a practical quantum computer. First, atoms change energy states very quickly -- much more quickly than even the fastest computer processors. Next, given the right type of problem, each qubit can take the place of an entire processor -- meaning that 1,000 ions of say, barium, could take the place of a 1,000-processor computer. The key is finding the sort of problem a quantum computer is able to solve.

If functional quantum computers can be built, they will be valuable in factoring large numbers, and therefore extremely useful for decoding and encoding secret information. If one were to be built today, no information on the Internet would be safe. Our current methods of encryption are simple compared to the complicated methods possible in quantum computers. Quantum computers could also be used to search large databases in a fraction of the time that it would take a conventional computer.

It has been shown in theory that a quantum computer will be able to perform any task that a classical computer can. However, this does not necessarily mean that a quantum computer will outperform a classical computer for all types of task. If we use our classical algorithms on a quantum computer, it will simply perform the calculation in a similar manner to a classical computer. In order for a quantum computer to show its superiority it needs to use new algorithms which can exploit the phenomenon of quantum parallelism.

The implications of the theories involved in quantum computation reach further than just making faster computers. Some of the applications for which they can be used are –

6.1 Quantum Communication

Quantum communication systems allow a sender and receiver to agree on a code without ever meeting in person. The uncertainty principle, an inescapable property of the quantum world, ensures that if an eavesdropper tries to monitor the signal in transit it will be disturbed in such a way that the sender and receiver are alerted.

The expected capabilities of quantum computation promise great improvements in the world of cryptography. Ironically the same technology also poses current cryptography techniques a world of problems. They will create the ability to break the RSA coding system and this will render almost all current channels of communication.

6.2 Artificial Intelligence

The theories of quantum computation suggest that every physical object, even the universe, is in some sense a quantum computer. As Turing's work says that all computers are functionally equivalent, computers should be able to model every physical process. Ultimately this

suggests that computers will be capable of simulating conscious rational thought. And a quantum computer will be the key to achieving true artificial intelligence.

7 References

[1] Glassner, Andrew S. "Quantum computing. 3" *Computer Graphics and Applications, IEEE*, Vol 21, pp 72 – 82, Nov/Dec 2001.

[2] Hughes, Richard J., Williams, Colin P. "Quantum computing: the final frontier?" , *Intelligent Systems and their Applications*,IEEE ,Vol15, pp 10-18, 2000.

[3] Glassner, Andrew S. "Quantum computing. 2" *Computer Graphics and Applications*, IEEE, Vol 21, pp 86 – 95, Sept/Oct 2001.

[4] Glassner, Andrew S. "Quantum computing. 3" *Computer Graphics and Applications, IEEE*, Vol 21, pp 84 – 92, Jul/Aug 2001.

[5] Narayanan, Ajit "Quantum computing for beginners", *Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on IEEE*, vol 3, 1999

Ms. Megha Khandelwal received her B.Tech degree from Uttar Pradesh Technical University. Currently she is pursuing her M.Tech in Computer Science and Engineering from Centre for Development of Advance Computing (CDAC), Noida.

Mr. Subho Sankar Chatterjee received his B.Tech degree from Uttar Pradesh Technical University. Currently he has completed his Masters in Business Administration in Finance from IBS Hyderabad, ICFAII University