Revealing New Concepts In Cpytography & Clouds

Vidhu Rawal, Ashutosh Dhamija, Sumit Sharma

Abstract— The following paper describes how quantum mechanics can be used to improve computation. The main challenge for a conventional computer is to solve an exponentially difficult problem and factoring a large number. In the course of this paper, the standard tools of computation, universal gates and machines are reviewed. These ideas are then applied first to conventional computers and then to quantum computers. A schematic model of a quantum computer is described as well as some of the subtleties in its programming.

Keywords— Controlling qubits, Decoherence, Cryptography, Superposition, Entanglement

1. INTRODUCTION

The broad umbrella of quantum computing covers ideas from classical information theory, computer science, and quantum physics. Information theory and quantum mechanics fit together very well. . The quantum entanglement and EPR-Bell correlations form the essential new ingredient which distinguishes quantum from classical information theory, and, arguably, quantum from classical physics. On the atomic scale matter obeys the rules of quantum mechanics, which are quite different from the classical rules that determine the properties of conventional logic gates. So if computers are to become smaller in the future, quantum technology must replace or supplement what we have now. The point is, however, that quantum technology can offer much more than cramming more and more bits to silicon and multiplying the clock-speed of microprocessors. It can support entirely new kind of computation with qualitatively new algorithms based on quantum principles!

So what is a 'Quantum Computer'? A *Quantum Computer* is a computer that harnesses the power of atoms and molecules to perform memory and processing tasks. It has the potential to perform certain calculations billions of times faster than any silicon-based computer. The classical desktop computer works by manipulating bits, digits that are *binary* -- i.e., which can either represent a zero or a one. Everything from numbers and letters to the status of your modem or mouse are all represented by a collection of bits in combinations of ones and zeros. These bits correspond very nicely with the way classical physics represents the world. Electrical switches can be on or off, objects are in one place or they're not, etc.

- Vidhu Rawal, Assistant Professor, ECE Deptt. JMIT, Radaur, vidhurawal@yahoo.co.in
- Ashutosh Dhamija, Assistant Professor, ECE Deptt. JMIT, Radaur, dhamija.ashutosh@gmail.com
- Sumit Sharma, Assistant Professor, ECE Deptt. JMIT, Radaur, er.sumitvashisht@hotmail.com

Quantum computers aren't limited by the binary nature of the classical physical world, however -- they depend on observing the state of *quantum bits* or *qubits* that might represent a one or a zero, 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.*

How does a quantum computer work? 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 qubit, exist in the classical '0' and '1' states, but it can also be in a superposition of both! In this coherent state, the bit exists as a '0' and a '1' in a particular manner. Let's consider a register of three classical bits: it would be possible to use this register to represent any one of the numbers from 0 to 7 at any one time. If we then consider a register of three qubits, we can see that if each bit is in the *superposition or coherent state*, the register can represent all the numbers from 0 to 7 simultaneously!

2. LITERATURE SURVEY

1965: Physicist Richard Feynman, involved deeply in the development of the first atomic bomb, proposes significant theories of quantum electrodynamics, a realm concerned with the way in which electrons interact with one another through the electromagnetic force propagated through the photon. Creating Nobel-winning, simple visual depictions of the possible interactions between an electron and photon and other atomic interactions.

1980: Feynman, among others, begins to investigate the generalization of conventional information science concepts to quantum physical processes, considering the representation of binary numbers in relation to the quantum states of two-state quantum systems.

1985: David Deutsch, of Oxford, publishes a theoretical paper describing a universal quantum computer, proving that if two-state system could be made to evolve by means of a set of simple operations, any such evolution could be produced, and made to simulate any physical system; these operations come to be called quantum 'gates', as they function similarly to binary logic gates in classical computers.

1994: *Shor's Algorithm*: Peter Shor, working for AT&T, proposes a method using entanglement of qubits

and superposition to find the prime factors of an integer, a rather valuable process as many encryption systems exploit the difficulty in finding factors of large numbers. In principle, his algorithm would far surpass the efficiency of any known computer when executed on a quantum computer.

1995: The National Institute of Standards and Technology and the California Institute of Technology jointly contemplate the problem of shielding a quantum system from environmental influences and perform experiments with magnetic fields, which allow particles (ions) to be trapped and cooled to a quantum state. This method, however, allows only devices of a few bits to be created, ones which lose coherence rapidly.

1996 *– present*: A team composed of University of California at Berkeley, MIT, Harvard University, and IBM researchers pursue a somewhat similar technique, but using nuclear magnetic resonance (NMR), a technology which seems to manipulate quantum information in liquids.NMR acts on quantum particles in the atomic nuclei of the fluid by creating a certain "spin;" the alignment of a given particle's spin betrays its value, 0 or 1. By varying the electromagnetic field used, certain oscillations are found which allow certain spins to flip between these states, allowing them to exist in both at once. Also, the constant motion of molecules in liquids create interactions allowing the construction of logic gates through NMR, the basic units of computation. The team develops a 2-bit quantum computer made from a thimble of chloroform; input consists of radio frequency pulses into the liquid containing, in essence, the compiled program to be executed.

1998: In 1993, the feasibility of quantum teleportation is proposed by an international team of researchers, who based their conclusions on a theorem of quantum mechanics called the Einstein-Podolsky-Rosen effect. The theorem describes how two particles which come into contact become "entangled," and part of the same quantum system. The group theorizes that two entangled, "transporter" particles introduced to a third, "message" particle might transfer properties from one to the other. The idea is actually put into practice nearly six years later, by researchers at the University of Innsbruck in Austria. Two pairs of entangled photons were exposed to each other, and it is revealed that the polarization state of one may be transferred to the other. The discovery possesses implications for data transfer and networking among quantum particles in quantum computing. Computing as we know it has existed for decades now, and existed for even longer in other forms, both realised and theoretical. The ones and zeroes that make up the binary system are ubiquitous. Quantum mechanics has also existed for decades, however it is only recently that scientists have begun to manipulate its weird and wonderful properties to achieve remarkable things. Even so, it was in the 1980s that someone first proposed the idea of a quantum computer, making use of some of quantum mechanics' more interesting properties.

3. QUANTUM CONCEPTS

1. Superposition

The primary effect which differentiates quantum computing from classical computing is known as "superposition". A classical bit exists in one of two states - as a zero, or as a one. A quantum bit, also known as a qubit, can make use of superposition to be in either a zero state, or a one state, or both - at the same time. This interesting ability was made famous by the "Schrdinger's cat" analogy, in which a cat in a sealed environment could be dead and alive at the same time. In a quantum computer, something similar occurs. A qubit (inside a sealed environment) is given a certain stimulus to enter a quantum state. When in this state it is possible to perform logical operations similar to those found in a classical computer on the qubit. When the qubit is read, or "measured", the qubit will collapse to a one or zero.

2. Entanglement

The second effect which is of importance is known as entanglement. Imagine a pair of qubits in the same system. Given the correct stimulus, they will both head into a quantum super positional state. In some cases, however, they will become entangled. What this means is that while in superposition the two qubits will remain entirely independent, but on measurement of one or both, the two become linked, and will always collapse to the same value as each other. This has some use in quantum computing, but comes into its own in communications, especially "quantum cryptography", which allows a sender and a recipient to communicate without actually sending the data via anything else.

a. Imagine two qubits, each in the state |0> + |1> (a superposition of the 0 and 1.) We can entangle the two qubits such that the measurement of one qubit is always correlated to the measurement of the other qubit.
b. To become entangled, two particles are allowed to interact; they then separate and, on measuring say, the velocity of one of them (regardless of the distance between them), we can be sure of the value of velocity of the other one (before it is measured).

3. Controlling Qubits

It is of course imperative that qubits can be altered, so that computation is made possible. But this needs to be done without measuring the qubit that needs altering, as this would cause it to collapse and destroy the quantum system. Traditional logic gates, like for example an AND gate, would cause this to happen. This is due to something known as reversibility - an AND operation is not reversible, since if it outputs a 0, it is impossible to tell which of the inputs were 0 or 12. As such, it is necessary to use reversible gates. One such gate is the CONTROLNOT gate, or CN gate. One of its inputs (the target) is inverted according to its other input (the controller). Note that while the controller needs to be a classical binary value, the target can quite easily be in a super positional state. If it is, the probability of its outcomes is inverted, rather than its actual value (this would be impossible since it actually has two values!). Similar operations on qubits are possible using other quantum gates or with rotation. Alternatively, think of the CN gate as having two outputs, outputting the result of inverting the target, if applicable, and passing the controller through unchanged. It can then be seen that the CN gate is reversible, since by reading the new target and the control bit, the original inputs can be determined. This behaviour in turn implies that the superposition of the target does not need to be destroyed in order to alter it.

4. The pitfall of quantum computing – Decoherence Consider a qubit that is in the coherent state. As soon as it measurable interacts with the environment it will decohere and fall into one of the two classical states. This is the problem of decoherence and is a stumbling block for quantum computers as the potential power of quantum computers depends on the quantum parallelism brought about by the coherent state. This problem is compounded by the fact that even looking at a qubit can cause it to decohere, making the process of obtaining a solution from a quantum computer just as difficult as performing the calculation itself. Even though we try to isolate the quantum system from the environment much as we can, we cannot supply total isolation. Therefore, the interaction of the quantum system and the environment result in "*Decoherence*" of the quantum state, which is equivalent to a partial measurement of the state by the environment.

4. APPLICATIONS

1. Quantum Cryptography

Since quantum computing is on the verge of breaking cryptography as we know it, it seems only right that it offers a replacement. Thankfully it provides a very good one, making use of entanglement, superposition, and the irreversibility of measurement to provide a tamper-proof method of communication. Suppose X wants to send Y a private message. The traditional method of accomplishing this is to encrypt the message with a key which only X and Y know. The trouble is getting the key from X to Y securely - if someone intercepts the key, they will be able to read all of their messages! One solution is to send the key using two entangled qubits. X sets up one of the qubits, and then sends a message to Y via classical means that the qubit is ready. He can now measure his qubit, which is entangled to X's, and he will have part of the key. It is still possible for an eavesdropper to read this data, if they also have a qubit which is entangled to the other two. However, by measuring the qubit, the quantum state collapses - when Y reads his qubit, it has already collapsed, which means that someone has intercepted part of the key. He should now send a response via the qubit to say that the communication has been compromised. If he did this via classical means, then the signal could be intercepted and altered, but not so with the qubit. Even if his response is intercepted, it is still obvious to X that the communication has been compromised. At this stage X can decide to use a new key, or perhaps break off communication until she feels more secure. The eavesdropper will have learned nothing.

2. Bioinformatics

A frightful possibility in the not too distant future is bio-engineered terrorism or accidents. Suppose someone were to engineer a very harmful germ and unleash it upon us. Bioinformaticists might be enlisted to analyze this germ, as their findings might help to find an antidote. Clearly, how long it takes to analyze the germ is critical in this scenario. One common tool in bioinformatics is MCMC(Bayesian network methods (a subset of which is MCMC (Markov Chain Monte Carlo) methods)), so if MCMC can be performed faster with a quantum computer than a classical computer, that would help bioinformaticists do their job more quickly.

3. Factorizing large numbers very rapidly (Shor's algorithm)

4. Intensive computations in areas such as astronomy, physics & chemistry.

5. Simulation of high computational models such as nuclear explosions and oil discovery.

6. 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.

5. CONCLUSION & FUTURE ASPECTS

With classical computers gradually approaching their limit, the quantum computer promises to deliver a new level of computational power. With them comes a whole new theory of computation that incorporates the strange effects of quantum mechanics and considers every physical object to be some kind of quantum computer. A quantum computer thus has the theoretical capability of simulating any finite physical system and may even hold the key to creating an artificially intelligent computer. The quantum computers power to perform calculations across a multitude of parallel universes gives it the ability to quickly perform tasks that classical computers will never be able to practically achieve. This power can only be unleashed with the correct type of algorithm, a type of algorithm that is extremely difficult to formulate. Some algorithms have already been invented; they are proving to have huge implications on the world of cryptography. This is because they enable the most commonly used cryptography techniques to be broken in a matter of seconds. Ironically, a spinoff of quantum computing, quantum communication allows information to be sent without eavesdroppers listening undetected. For now at least, the world of cryptography is safe because the quantum computer is proving to be very difficult to implement. The very thing that makes them powerful, their reliance on quantum mechanics, also makes them extremely fragile. Although the future of quantum computing looks promising, we have only just taken our first steps to actually realizing a quantum computer. There are many hurdles, which need to be overcome before we can begin to appreciate the benefits they may deliver. Researchers around the world are racing to be the first to achieve a practical system, a task, which some scientists think, is futile. *David Deutsch* - one of the groundbreaking scientists in the world of quantum computing - himself said, "Perhaps, their most profound effect may prove to be theoretical".

Can we really build a useful quantum computer? Who knows; in a quantum world, anything is possible!

"Quantum computing could head to 'the cloud' "--BBC NEWS (9th Jan 2012)

Quantum computing will use the inherent uncertainties in quantum physics to carry out fast, complex computations. A report shows the trick can extend to "cloud" services such as Google Docs without loss of security. This "blind quantum

computing" can be carried out without a cloud computer ever knowing what the data is. Quantum computing has been heralded as the most powerful potential successor to traditional, electronics-based computing. One of the peculiarities of the branch of physics called quantum mechanics is that objects can be in more than one state at once, with the states of different objects tied together. Instead of the 0 and 1 "bits" of digital computing, quantum computing aims to make use of these mixed and entangled states to perform calculations at comparatively breathtaking speeds.

6. REFERENCES

[1] http://www.ibmpressbooks.com/articles/article.asp?p=374693&seqNum=6

[2] http://www.economist.com/node/21548151

[3] Bub, J. (2006a), 'Quantum information and computation'

[4] Hodges, A. (2005), 'Can quantum computing solve classically unsolvable problems?'

[5] https://cryptoanarchy.org/wiki/Quantum_computer

[6] Deutsch, D. and Jozsa, R. (1992), 'Rapid solution of problems by quantum computer', *Proc. Roy. Soc. Lond*, A 439: 553–558.

[7] http://ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm

[8] http://www.bbc.co.uk/news/science-environment-16636580

[9] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/

[10] http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology.htm

[11] http://qbnets.wordpress.com/2009/08/28/military-uses-of-quantum-computers/

[12] http://news.discovery.com/tech/quantum-computer-120220.html

[13] CNet News - "Start-up demos quantum computer" - http://news.com.com/Start-up+demos+quantum+computer/2100-1008_3-6159152.html - last accessed 31st May 2007.