Quantum Computers: A New Paradigm in Information Technology

Mahesh S. Raisinghani
Graduate School of Management, University of Dallas, Texas
mraising@gsm.udallas.edu

"Our greatest glory is not in never failing but in rising up every time we fail"
-- Ralph Waldo Emerson

Abstract

The word 'quantum' comes from the Latin word quantus meaning 'how much'. Quantum computing is a fundamentally new mode of information processing that can be performed only by harnessing physical phenomena unique to quantum mechanics (especially quantum interference). Paul Benioff of the Argonne National Laboratory first applied quantum theory to computers in 1981 and David Deutsch of Oxford proposed quantum parallel computers in 1985, years before the realization of qubits in 1995. However, it may be well into the 21st century before we see quantum computing used at a commercial level for a variety of reasons discussed in this paper. The subject of quantum computing brings together ideas from classical information theory, computer science, and quantum physics. This paper discusses some of the current advances, applications, and challenges of quantum computing as well as its impact on corporate computing and implications for management. It shows how quantum computing can be utilized to process and store information, as well as impact cryptography for perfectly secure communication, algorithmic searching, factorizing large numbers very rapidly, and simulating quantum-mechanical systems efficiently. A broad interdisciplinary effort will be needed if quantum computers are to fulfill their destiny as the world's fastest computing devices.

Keywords: quantum computing, qubits, applications of quantum computing, challenges facing quantum computing

"Let chaos reign. Resolution comes through experimentation. Only stepping out of the old ruts will bring new insights."

---Andrew Grove, Chairman, Intel

Introduction

In the last few years, the theoretical study of quantum systems serving as computational devices has achieved tremendous progress. An understanding of quantum mechanics has been absolutely central to today's high-tech, wired world. Without it, computers, television, satellites, telephones and most other modern gadgets would probably not be as sophisticated and plentiful as they are now. The subject of quantum computing

brings together ideas from classical information theory, computer science, and quantum physics. *Information* is something that can be encoded in the state of a physical system, and a *computation* is a task that can be performed with a physically realizable device. Therefore, since the physical world is fundamentally quantum mechanical, the foundations of information theory and computer science should be sought in quantum physics.

Imagine a computer whose memory is exponentially larger than its apparent physical size or a computer that can manipulate an exponential set of inputs simultaneously. Relatively few and simple concepts from quantum mechanics are needed to make this concept of quantum computers a possibility. A quantum system is in general not in *one* "classical state", but in a "quantum state" consisting of a *superposition* of many classical or classical-like states. In fact, quantum information -- information stored in the quantum state of a physical system -- has weird properties that contrast sharply with the familiar properties of "classical" information.

The quantum computer -- a new type of machine that exploits the quantum properties of information -- could perform cer-

tain types of calculations far more efficiently than any fore-seeable classical computer.

In describing a computer as a cup of coffee one may be doing so literally since the new computer of tomorrow might be based on molecules in a liquid instead of silicon. This may prove to be a paradigmatic shift in the way we manage information technology today.

Evolution of Computers

As civilization marched forward in search of better ways of doing things, the various physical resources, such as materials, forces and energies, were exploited for their potentials. From the gears of the first Pascal calculating machine in 1642, to the relays and valves of the first decoder in WWII made by Great Britain, to the transistors and integrated circuits of today, the ever-shrinking computer brought forth improvement in speed and functionality. A state-of-the art IBM chip with 0.25 micron features contains 200 million transistors. That single chip is sized about ¼ of a penny. Present 'state-of-the-art' components possess features only a few hundreds of nanometres across (a nanometre is a thousandth of a micron, or a billionth of a metre).
(http://www.qubit.org/intros/nano/nano.html , 2000).

Limits In Miniaturization

The continual miniaturization of the transistor over the last few decades has enabled computing power to double every couple of years. As transistors became smaller more could be integrated onto a single chip. However, this miniaturization is now reaching a limit set by nature: a quantum threshold below which principles of transistors will no longer hold true. In other words, there is a limit to the miniaturization of a computer based on silicon. Also one of the difficulties with the program of miniaturizing conventional computers in trying to build a classical computing machine on such a small scale is the difficulty of dissipated heat. If these chips were to be miniaturized further to the scale of tens of nanometres then their operation would be disrupted by the emergence of quantum phenomena, such as electrons tunneling through the barriers between wires. In order to improve upon the speed and power of computing an alternative technology must be found. (Braunstein, 1995; Gershenfeld and Chuang, 1998; Verrengia, 2000).

Quantum Computers: Antecedents and Taxonomy

The word 'quantum' comes from the Latin word quantus meaning 'how much'. Quantum is a discrete quantity of electromagnetic energy (photon) which can be released when an electron is activated, or when a radioactive chemical element drops from a higher to a lower energy level. The quantum is the smallest possible amount of energy at a given frequency.

The reference discipline is quantum mechanics, a field that has led to the development of high-speed optical neurocomputers that can use multiple quantum-well structures (MQWS) that consist of aluminum gallium arsenide layers only several atoms thick. These are sandwiched (alternated) between wider gallium arsenide layers that are 30 atoms thick. This alternating structure is called a tunneling biquantum-well. Optical images are captured, stored, and read by the use of optically-addressable spatial light modulators (SLM) which use ferro-electric liquid crystals (FLC). FLC-SCM can operate at 50 microseconds with a spatial resolution of 40 line-pairs per millimeter. These enable a 1-square centimeter device to function at 3.2 giga operations (10^9) (PricewaterHouse, 2000).

Almost all of today's computers are based on simple Turing Theory and employ Boolean logic based on binary mathematics. Even "parallel" computers are really complex Turing engines employing multiple computing modules that deal with pieces of incoming data (chunks, bytes, instructions, etc.). There has been some research into biological computing using enzymes or large-molecule systems as memory, shift registers, etc., but this has not proven to be very practical.

Classical Computers vs. Quantum Computers

The first generation of nanocomputers will have components that behave according to quantum mechanics, but the *algorithms* that they run will probably not involve quantum mechanics. We might call such computers 'nanometre-scale *classical* computers' (here the word 'classical' means 'not quantum'). But scientists have recently realized that there is another, more exciting possibility - quantum mechanics might be used in an entirely new kind of algorithm that would be fundamentally more powerful than any classical scheme. A computer that could run such an algorithm would be a true 'quantum computer'
(http://www.qubit.org/intros/nano/nano.html).

Quantum computers are superior to classical computers in several ways, one of which is that it processes information in a parallel manner. However, unlike conventional massively parallel systems that have many processors working in parallel, there is only a single quantum processor. This desirable characteristic is the driving force behind increased computing power and is the basis for supercomputers of today. Supercomputers combine miniaturization with parallel computing. Supercomputers coax multiple processors to carry out multiple operations simultaneously. However, improvements in such design expose a fundamental flaw: the logic built into

processors is inherently serial and tasks have to be carried out one step at a time. In essence, multiple processors speed up the serial process by dividing work amongst them. However, the complexity and inefficiency of such design in supercomputers lead to high costs that are hard to justify, yet those computers still have trouble with tasks such as predicting the national economy. A truly parallel computer will have simultaneity built into its very nature. It would allow operations on multiple instances of events at the same time. In essence, this is the key concept of a quantum computer.

A Closer Look Inside Quantum Computers: Quantum Fundamentals

To better explain what makes quantum computers so different from the computers today one must begin by looking at the basic chunk of information – a Bit. This code represents and communicates the present state of the system. In today's computer, the voltage between the plates in a capacitor represents Bit information. A charged capacitor denotes Bit value 1 and an uncharged capacitor denotes Bit value 0. This information can also be encoded in two different states of an atom. However, in quantum mechanics an atom can also be prepared in *coherent superposition* of the two states, making it exist in both the state of 0 and state of 1 (as both Bit 0 and Bit 1).

Quantum computing is based on a different physics than digital computing. Instead of having two (or three) states-per-element like digital computers that are off, on, or neither, quantum computers can have all three states at the same time. An 8-bit digital computer can exist in only one of 256 states at a time while an eight bit quantum computer can exist in all 256 states at a time and theoretically, work on 256 calculations at once (quantum parallelism). Each of the 256 numbers in this 8-bit example has an equal probability of being measured so that a quantum processor functions as a random number generator. The actual register is representing all of these values at once but a single value output only occurs at measurement. While a classical digital computer would have to operate on each number from 0 to 255, quantum computers require only one pass through the "processor", radically reducing calculation time. Of course, the larger the register size, the larger the number - even a simple 10-bit quantum computer could scream past a supercomputer.

Where the digital computer uses binary digits (bits), the quantum computer uses qubits, but qubits are extremely difficult to generate. A quantum switch must be undisturbed. Light, molecules, or impinging fields required for the proper operation of a quantum computer depend on the interaction of the various qubits without any outside influence. When disturbed, the qubit becomes quite Newtonian rather than quantum and

selects a definite state - by chance becoming, dare we say, digital (Smalling, 2000).

Quantum Computing Applications

The realization that quantum computers harness so much power has touched off a storm of research and studies for possible applications, one of which is its ability to search for data. A classical computer can search a list of y data items in y/2 steps. A quantum computer takes in general [square root (y)] steps. A quantum computer can search a million-name phone book for a number in 1,000 tries instead of half a million or slightly less tries if using a binary search (assuming that it is alphabetized), and does it much faster too. The same power can be used to search every nook and cranny of the Internet in half an hour or less. Quantum search algorithm is good for more than merely looking up phone numbers. The way a quantum computer conducts a search can be compared to finding a ball hidden beneath one of several given cups by checking all the cups simultaneously – a parallel process that is made possible by quantum mechanics (PricewaterhouseCoopers, 2000). It can search through items not explicitly spelled out on a list. It can take a brute-force approach to any problem whose potential solutions can be systematically itemized, trying them all until it finds a solution that works. Non-quantum versions of the brute-force approach are very commonplace in the world of computing – in gamming programs such as chess. Because of its speed and versatility, it seems likely that the search aspect of quantum computers will be one of the more important applications of a quantum computer.

By the laws of quantum physics, specifically the Superposition Principle, atoms can be in several different energy states at once. The enormous potential of quantum computing is derived from the fact that this principle could allow for the creation of a computing device able to act on all its possible states simultaneously, carrying out numerous computations in parallel. Quantum computers are able to perform nonclassical logic operations and can be used to solve computationally intractable problems that cannot be solved by conventional massively parallel supercomputers (PricewaterhouseCoopers, 2000)

Data Encryption

One application for the quantum computer may be in the field of encryption. Encryption is used in data protection schemes to protect sensitive information in the financial world. Encryption techniques of today would be rendered obsolete since quantum computers factor large numbers quite easily and would be able to crack anything but quantum codes (Price, 2000). Encryption is based on one simple fact – the extreme difficulty in factoring integers. An example would be to com-

pare multiplication between two integers: 191 and 211. The result is 40,301. However, factoring 40,301 is very difficult in comparison. In fact, the difficulty in factoring integers grows exponentially as the number of integers involved increases. The largest number that has been factorized by a supercomputer has 140 digits. A typical system password is around 100 digits for ease of manipulation. (Lov, 1999), chosen in part due to the difficulties involved in factoring or breaking the code. A similar scheme is used in devising public/private keys for secure information transmissions such as making purchases over the Internet. Using a quantum computer, however, one can factor the "key" containing 400 digits in about a year (Gershenfeld, et al., 1998) where as a supercomputer would take much more than the estimated age of the universe.

Other Scientific Calculations

Calculations that would strain the capacities of the best and fastest machines such as modeling the economy, forecasting the weather and high mathematical function calculations would be quite easily done using quantum computers.

Challenges Facing Quantum Computers

A quantum computer will be much more vulnerable than a conventional digital computer to the effects of noise and of imperfections in the machine. Unavoidable interactions of the device with its surroundings will damage the quantum information that it encodes, a process known as decoherence. Schemes must be developed to overcome this difficulty if quantum computers are ever to become practical devices. However, quantum error-correcting codes can be exploited to protect quantum information from decoherence and other potential sources of error and enable a quantum computer to perform reliably despite the inevitable effects of noise. Due to their multiple states (unlike two-state digital processes) quantum computers will have some of the problems that analog computers had - namely error correction and calculation reliability.

Simple quantum computers with 3 qubits have already been built, but some scientists are pessimistic about more complex ones due to difficulties in controlling atomic sized particles and problems caused by interaction with the environment. There are practical difficulties when engineering interactions between qubits, working at single-atom and single-photon scales not withstanding. Quantum computers are also extremely fragile. The slightest interaction with everything outside the system will destabilize superposed state of quantum bits. Shielding from heat, cosmic rays and even outside observers. Also, the act of reading out an answer from a quantum computer using an uncontrolled external system destroys

the system by virtue of quantum mechanics and one would need to re-program.

Since these errors cannot be completely avoided, finding a reliable way to correct them is necessary. Answers are emerging that include using extra quantum data and performing error-correcting algorithms on the qubits. Researchers at Los Alamos National Laboratory have developed an error-correction system in which each encoded qubit is checked for errors, encoded, and then multiplied five times. Nuclear magnetic resonance (NMR) is being used to encode the quantum data-by putting a certain spin on nuclei-and its use is helping to eliminate observation-related data corruption (Pricewater-houseCoopers, 2000).

Due of their multiple states (unlike two-state digital processes) quantum computers will have some of the problems that analog computers had - namely error correction and calculation reliability (although this does not sound very quantum mechanical). The verdict has not been read on what type of error correction will work with qubits and quantum measurement in general. However, the research on new forms of calculation, error correction, and algorithm construction will improve the state of digital computing, data compression, and error correction.

Implications for Management

Given the vast computing power an individual may have access to in an office space, managing the IT department may prove exceedingly difficult in terms of user service versus efficiency. A user liaison unit may be unavoidable to ascertain just what the user may or may not need/access. The organization structure may be determined by the constantly changing needs as future tasks will be completed much faster than tasks today. As resources shift from place to place the IT manager will be called upon to advise on making the organizational structure more flexible and adaptable. The IT department will also need to monitor end-users closer – the approach of *let them sink or swim* may no longer apply. Instead, more rigid controls may need to be put in place to control equipment use and information flow.

Security

Information Systems, especially legacy systems may be more vulnerable to various computer crimes. The leap in computing power may create a big gap between businesses equipped with the latest technologies and those who aren't. Those businesses that lag behind will be a lot more vulnerable to attacks such as data tempering and viruses. Since quantum computers are especially sensitive to changes in the environment, I think it's entirely possible for hackers to disable or damage systems

not just through software but also through magnetic disturbances, heating the environment, etc. Prevention will be ever more counted upon as a major role of any IT department. In addition, prevention against inadvertent damage to systems might be required. More layers of security measures such as tougher access control and new encryption schemes may be needed to guard against computer criminals than ever before. For the IT department, it would not be surprising to see a specialized position created within the realm of managing information systems: that of an Information Security Manager. This position may last at least until the gap between legacy technologies narrows to a more manageable size.

Technology Integration

Difficulties in integrating legacy equipment into the new systems will be substantial, not taking into consideration assimilating other nanotechnologies such as DNA computers. The following is a list of important measurements that should be taken into consideration while trying to determine what the best course of action may be:

> Number of cross functional activities.
> Number of system that will benefit from quantum technology.
> Number of systems that are suitable for business reengineering.
> Number of silicon based computers/systems.
> Number of other nanotechnologies (nonquantum).
> Number of suppliers using legacy systems.
> Amount of resources available for investment.
> What are the organizational goals?
> What organizational structure changes are forecasted?
> Number of customers using legacy systems.
> State of the current security measures.

Each of the items above may be assigned a numeric grade and weighted according to pre-determined scale. The outcome may be used to determine:

> Replacement of all old systems immediately.
> Gradual replacement over a period of time.
> Keep localized legacy systems.

It is pertinent to realize that the benefits of a quantum computer system are likely to increase as technology advances and becomes more mature. However, there will be an initial investment and adjustment period where cost does not justify demand. This is temporary in nature, but exaggerated expectations and poor integration planning may spell doom for the introduction of the system.

Implications for Corporate Computing

Perhaps the most important effect that quantum computing may bring forth, is the coming full circle back to a time where the small company, or even the inventor, can develop methods and equipments that significantly affects the way things are done. No more will one need huge quantities of capital or resources or access to supercomputers in order to model his/her ideas. It will be a world of single desktop systems, lone developers and their imagination changing the universe.

Quantum computers are extremely fragile and the slightest interaction with elements outside the system can destabilize superposed state of quantum bits. Since quantum computers are especially sensitive to changes in the environment, it is quite possible for hackers to disable or damage systems not just through software but also through magnetic disturbances, heating the environment, and so forth. Also difficulties in integrating legacy equipment into the new systems can be substantial, notwithstanding assimilation of other nanotechnologies such as DNA computers.

Future Trends

Carver Mead, a visionary of computer hardware design, has pointed out that until lately, advances in hardware have focussed on issues of scale; smaller is better, smaller is faster (Mead, 1989). But he points out that although the brain's hardware is of much larger scale, and much slower than current computer hardware, the brain can perform computations far beyond our fastest supercomputers. His recommendation, then, for advances in hardware design, is to look at how the brain is organized, for inspiration to come up with new forms of computation, rather than just try to make the kinds of computer we have now faster and smaller. Neural network algorithms are part of this search for novel kinds of computation. A computer on the spatial and temporal scale of quanta is bound to have advantages over current hardware, but Mead's point still holds. So why not pursue both improvements in scale and alternative forms of computation? That is one of the reasons for looking at quantum learning; but perhaps there are qualitative advantages of quantum learning that are not just the simple addition of algorithmic and scale advantages.

It will be the responsibility of the IT Manager to set realistic goals and expectations that are achievable. Too often there exists high expectations for new technologies that tends to discourage managers and users alike after the initial euphoria wears off. Heightened expectations can also cause the technology to fail.

Quantum computing devices are probably still several decades away, but advances and research that might make quantum-

computing possible already are taking place. True quantum computers are many years from being able to compete with classical computers. When their properties are fully understood, simple quantum computers will help improve classical computation, lending themselves to the creation of integrated circuits containing molecular-size components. The use of quantum logic devices would make it possible to fit 1 trillion devices on a 1 cm2 chip, as opposed to a mere 6 million per chip in 2000 (PricewaterhouseCoopers, 2000).

When is the next milestone expected in this area? Japanese and American computer manufacturers are currently working on a new level of technology that may supersede current supercomputers and launch a new era of optical computing using opto-electronic integrated circuits (OEIC). These will be used in optical neuro-computers (ONC) with switching devices topping speeds of 1 picosecond (10 to the power of 12 seconds), operating at 1 gigahertz (10 to the power of 9). The fast speed of ONCs is due to the use of multiple quantum-well structures (MQWS) described in response to q.1. above. The Japanese Ministry of International Trade (MITI) claims that electronics has been the science of the 20th century, and that optics will be the science of the 21st century.

Conclusion

Perhaps the most important effect this new technology may bring forth, is the coming full circle back to a time where the small company, or even the inventor, can develop methods and equipments that significantly affects the way things are done. No more will one need huge quantities of capital or resources or access to supercomputers in order to model his/her ideas. It will be a world of single desktop systems, lone developers and their imagination changing the universe. It may be another two decades before we see quantum computing used at a commercial level but there is little doubt that the research on new forms of calculation and error correction will improve the state of digital computing, data compression, and error correction.

As Pamela McCorduck points out, "Word literacy has given us power…Computer literacy opens still another world, one that all eventually may enter as routinely as they enter the world of letters..." A broad interdisciplinary effort will be needed if quantum computers are to fulfill their destiny as the world's fastest computing devices.

References

Barenco, A. (2000). *A Short Introduction To Quantum Computation.* Center for Quantum Computation. Accessed July 2, 2000 at http://www.qubit.org/intros/comp/comp.html

Benjamin, S., & Ekert, A. (2000). *A Short Introduction To Quantum-Scale Computing*. Centre for Quantum Computation. Accessed September 27, 2000 at http://www.qubit.org/intros/nano/nano.html

Braunstein, S. (1995). *Quantum computation: a tutorial*. New York: Academic Press.

Gershenfeld, N. & Chuang, I. (1998). *Quantum Computing with Molecules.* Scientific American Internet Edition. Last Updated September 12, 1998 at http://www.sciam.com/1998/0698issue/0698gershenfeld.html#authors

Grover, L. (1999). Quantum Computing. *The Sciences*, July/August, 24-30.

Lloyd, S. (1995). Quantum-Mechanical Computers. *Scientific American*, 273 (4), 140-145.

Mead, C. (1989). *Analog VLSI and Neural Systems*. New York: Addison Wesley.

Norton, P. (1997). *Inside the PC* (7th ed.). Indianapolis, IN: Sams Publishing.

PricewaterhouseCoopers (2000). *Technology Forecast: 2000*. California: PricewaterhouseCoopers Technology Centre.

Smalling, E. (2000). *A Brief Overview Quantum Computing.* Accessed September 25, 2000 at http://www.connect.net/smalling/quantum1.htm

Verrengia, J. (2000). *Scientists Eye Quantum Theory Codes.* Yahoo Internet News, Accessed April 28, 2000 at http://dailynews.yahoo.com/h/ap/20000428/sc/uncrackable_code_2.html