Communications Research Centre Canada
An Agency of Industry Canada

Centre de recherches sur les communications Canada
Un organisme d'Industrie Canada

An Introduction to Quantum Computing Concepts

Quantum Computers versus Conventional computers

Don Olcheski, PESO

CRC Report No. CRC-TN-2008-003
Ottawa, April 2008

Caution

This information is provided with the express understanding that proprietary and patent rights will be protected.

An Introduction to Quantum Computing Concepts

Historical Perspective

In 1900, physicist Max Planck proposed that energy was not emitted in a continuous manner as theorized by classical physics, but rather in discrete packets or quanta. This became the basis for quantum theory. A single object in the quantum realm can exist in physically different states simultaneously, evolve in multiple ways simultaneously, and influence other quantum objects with no direct interaction.

Quantum computing uses the properties of quantum physics to perform calculations. The basic unit of computation used it is the qubit, or quantum bit. Unlike classical bits the qubit is not just 0 or 1 but is the superposition of both. In other words, it is both on and off at the same time.

Quantum computers are machines based on the principles of quantum mechanics, a branch of physics that describes the lesser-known world of subatomic particles where both a yes and no can simultaneously be true.

Quantum Computers versus Conventional Computers

Today's digital computers are constructed from transistors.
The transistors in today's digital computers hold information in binary units – either 1 or 0.

Quantum computers differ from conventional computers in that the fundamental information storage device on a chip is generalized from being exclusively "on" binary 1 or "off " binary 0 to a state where both states can co-exist (i.e. can be both on and off simultaneously). A device allowing this co-existence is called a *quantum bit or qubit*. The co-existence of two states in a one-qubit device leads to the key enabling property of a quantum computer. That capacity is the heart of the vast potential power of quantum computers.

Consider the difference between a 4-bit classical computer and a 4-bit quantum computer. The former can hold any one of 16 different numbers (0000 through 1111). The latter can hold all these numbers simultaneously. Assuming we would want to find the factor of a specific 4 bit number like say (1111) or in the decimal system 15 (see Appendix A).

Classical computing requires we perform 16 different operations (i.e. dividing the specific number by each of the possible factors, 0000 through 1111, and looking at the results) which in this case are 3 and 5. Conversely, with a quantum computer, we can do the same calculation in a single operation, given that a 4-qubit device holds all the possible 16 factors simultaneously. The factors 3 and 5 reveal themselves in one cycle. All this is required is to get the final answer to reveal itself in the classical world (a process called decoherence).

Advantages of Quantum Computing

To illustrate the potential advantages of quantum computing let us consider one problem challenging pharmaceutical researchers that is to predict the properties and behavior of a caffeine molecule, which contains 102 electrons. This solution requires solving an algorithm for 102 electrons. This requires the storing and processing of 2 to the power of 102 classical bits of information. This number is very large. The only method currently available is to actually build the molecules and observe their properties in nature. The invention of quantum computers that are able to simulate the property and behavior of molecules therefore promises to fundamentally change the way substances are designed at the molecular level. Dr. R. Laflamme (presently at the University of Waterloo - IQC) confirmed this concept in 2001.

Moreover computing capacity based on multi-qubit computer scales up exponentially, a fact that underlies the potential of quantum computers. For example 2 to the power of 3 equals 8 but scale your quantum computer to a 8 bit device and 2 to the power of 8 is 256 - so a 8 qubit quantum computer can theoretically process information at 256 times the speed of a classical computing model. While the classical digital byte can store any number between 0- and 255 using all of its 8 bits, it can only represent only one of those numbers at a time, say 10101010, but a qubit can be all of the numbers. Harnessing such scalability could solve the caffeine molecular problem above which is not possible using conventional parallel computing methods.

This technique allows much more information to be stored on a quantum bit than a classical bit, and allows massively parallel processing on a quantum scale. One calculation can give the answer for all the numbers on the byte at the same time. In other words for each clock cycle a quantum computer could perform 256 calculations in the same time a digital computer can perform just one.

However, problems arise when it comes to reading the information back. Any interaction with the environment – including trying to read the information stored – affect the qubits so that they change from a pure quantum state to a mixed state. This is known as decoherence and any reading taken from this state will be wrong. Various techniques are being developed to avoid *decoherence*

Given the ability to assemble and manipulate particles at the atomic level is the basis of nanotechnology, it is clear that a quantum computer could provide a dramatic boost to this area of technological development, amongst others which we will describe later, i.e. Cryptography.

Techniques to Obtain Quantum Information

There are several different approaches to obtain quantum information such as using laser pulses to force the interaction of photons that can contain quantum information. However, optical quantum computing schemes are not regarded as the most practical alternative. Another technique is the control or suppression of cooling an atom. One candidate according to some researchers in the field for building workable quantum computers is based on trapped ions, which are charged atomic particles that can be confined and suspended using electromagnetic fields.

In Canada and Europe there are several types of superconducting qubits (quantum bits). One of the common ones is the so-called flux qubit. It consists of a super-conducting ring with several small junctions (Josephsen) that are biased with a magnetic flux. In this regime the classical states are characterized by circulating persistent currents either clockwise or anti-clockwise. These currents can be detected with a sensor that detects the generated magnetic flux (see Appendix B).

In Canada, D-Wave of Vancouver, BC focuses exclusively on superconductor based hardware. *Superconductivity* is the phenomena wherein the electrical resistance of the metal disappears when the metal is cooled to low temperatures, near absolute zero.

There are three other platforms that are competitive to superconductors.

- Linear-optical,
- Semiconductor-based,
- Atom trap-based quantum computers

Leading Applications for Quantum Computing Technology

One of the current applications seeking deployment is *"Quantum Cryptography Systems and Communications"* (i.e. impregnable data encryption systems). Quantum cryptography systems would allow users to overcome the vulnerabilities of the public-key cryptosystems now widely deployed in business and government organizations such as the military to secure sensitive information from eavesdroppers.

The current approach in public-key systems deploys use algorithms to encrypt and decrypt data. The cryptosystems send a set of specific parameters – called a key – together with the plain-text information to be scrambled as input to the encrypting algorithm. They generate public keys that senders can use to encrypt a secure message. The receiver such as a bank then decrypts the message with a private key. The security of the key relies on randomly chosen long string of bits. But new algorithms or a powerful computational device that can factor the number into two smaller numbers can eventually break such codes.

As referred to above, current communications security is based on mathematical assumptions. The problem is that we do not know if these assumptions are correct. Quantum cryptography takes another approach. It bases security on a fundamental, quantum physical laws.

Quantum cryptography creates and sends code made from a series of individual photons with different polarizations or other properties. The direction in which the photon's electric field vibrates represents the 1 and 0 s of the computer language.
Quantum Cryptography relies on the inevitable modification of individual particles when someone tries to gain information about these properties. Hence if we first send a key to our business partner, and we encode this key into say light particles, we can find out if somebody tried to listen in.

conversely, we can also see when nobody tampered with the key, in which case we can use it to lock our message in a proven secure way.

Quantum Information Processing

Quantum information-processing concepts have the potential to create a revolution in computer science. Quantum mechanics explains the behavior of the building blocks of all matter and energy, such as photons, electrons and atoms. A niche example of quantum information processing is described in the analysis of the caffeine molecule referred to above. The Universite of Montreal has eminent faculty dedicated to this research (See Appendix D).

Summary

In this brief overview we have attempted to show that the if the exponential speed of the quantum computing device or machine can be harnessed, and when this occurs - it will make possible exciting applications that are incapable of being modeled and simulated using today's conventional technologies.

CRC
Business Development Office
613-998-2715

November, 2008

Appendix A

The binary (base two) numeral system has two possible values, represented as 0 or 1, for each place-value. In contrast, the decimal (base10) numeral system has ten possible values (0,1,2,3,4,5,6,7,8,9 for each place- value

The Table below is used to make the Binary to Decimal Conversion

2° = 1
2^1 = 2
2^2 = 4
2^3 = 8
2^4 = 16
2^5 = 32
2^6 = 64
2^7 = 128
2^8 = 256

To derive the binary - decimal equivalent for example using binary number 1111

From the Table above add the respective values

1+2+4+8 = 15 (decimal value)

For an 8 bit or one byte value

11111111

becomes:

1+2+4+8+16+32+64+128 = 255

10000000 = 128

Bit to Byte Conversions

A byte is a basic unit of measurement of information storage in a classical computer. There is no standard but a byte most often consists of 8 bits. The word "Byte" has two closely related meanings:

- A contiguous sequence of a fixed number of bits.
- A contiguous sequence of bits within a binary computer that comprises the smallest addressable word–size.

Because of computer architecture, bytes are always some multiple or exponent of 2. In the cases when used to describe data storage bits/byte are calculated as follows:

- 1 byte = 8 bits
- 1 kilobyte = 2^10 bytes = 1,024 bytes
- 1 megabyte = 2^20 bytes = 1,048, 576 bytes
- 1 gigabyte = 2^30 = 1,073,741,824 bytes

In Data Communications, a kilobit is a 1,000 bits. It is commonly used for measuring the amount of data that is transferred in a second between two telecommunications points.
Although the bit is a unit of the binary number system, bits in data communications are discrete signal pulses and have historically used the decimal number system. For example a modem capable of 28.8 kilobits per second is 28,800 bits per second.

According to the Institute of Quantum Computing (IQC) they describe a generic quantum state as an exponential number of classical states.

To represent one quantum bit you need 2 numbers (1,0).
Two quantum bits you need 00,01,10,11 thus 4 numbers.
Three quantum bits 000,001,011...111 needs 8 numbers
Four quantum bits needs 16 numbers
10 qubits needs 2^10 which is about a kilobit (1024 bits)
20 qubits needs 2^20 which is about a megabit (1,048,576 bits)
30 qubits needs 2^30 which is about a gigabit

Appendix B

Quantum Computer Hardware and Qubit Manipulations

Flux qubits encode information in the direction of circulating current around the qubit loop, which can be either clockwise or counter-clockwise. This current is quantized, and has a magnitude around one micro-amp. The magnetic flux threading the qubit loop, generated by this current, is also quantized.

A clockwise circulating current generates magnetic flux pointing down through the qubit loop. This we define to be the state corresponding to the binary zero (0). If the current is counterclockwise, it generates magnetic flux in the opposite direction. This corresponds to the qubit being in a binary state one (1).

Qubit Manipulation

If we place a superconducting wire near the qubit loop, and send current through the wire, we generate a magnetic field that the qubit (where the qubits could be niobium split junction devices about 10 by 10 microns in area) senses. This wire is called a bias wire generating a magnetic field. By varying the strength and direction of the current through the bias wire can manipulate the state of the qubit. This is because the qubit behaves like a magnet in the magnetic field created by the bias wire. A compass works on this principle where its direction can be affected by the changing magnetic field. So too can the (quantum) state of the qubit, via the magnetic field it generates, be affected by the magnetic field of the qubit bias wire.

Topics such as qubit initialization, qubit readout, coupling two qubits and running a calculation are beyond the scope of this paper and for further information please refer to the author for more details.

Appendix C

Research Chair in Quantum Computation

University of Waterloo
Natural Sciences and Engineering
519-888-4021

Michele Mosca
mmosca@iqc.uwaterloo.ca

Research involves

Reformulating the theory and practice of information processing in a quantum mechanical framework.
Developing the capabilities, and understanding the limitations, of information processing (including computation, communication and information security) in our quantum world.

Security in a Quantum World

One of the most pressing issues in the Information Age is ensuring that the information stored on our computers or transmitted to our colleagues, suppliers, customers, and others, is protected from unauthorized people. Not surprisingly, the sector of the communications industry that develops means of protecting information has grown in parallel with the spread of the Internet and private data networks. The spread of the Internet and the growth of so-called e-commerce have, in fact, been fuelled by the invention of public-key encryption, which relies on the intractability of computational problems like factoring large integers and finding discrete logarithms in specific groups. But, while there are no known efficient algorithms that run on classical computers for solving these computational problems and cracking public-key encryption, it has been shown that quantum computers can be used to defeat these systems.

Building on considerable expertise in the field of quantum computation theory, Dr. Mosca will pursue complementary tasks of finding new quantum algorithms and studying the limitations of various algorithmic approaches. In addition to determining the capabilities of quantum computers, Dr. Mosca believes that it is equally important to understand their limitations. By understanding where quantum computers are not advantageous, it is easier to focus energy in finding tasks for which they are suited. In addition, it is important to discover what types of cryptographic applications will be intractable even for quantum computers.

Collaboration is a key part of this research approach. As well as working in concert with collaborators across Canada and abroad, Dr. Mosca anticipates significant collaboration with Dr. Raymond Laflamme, another leading theorist in quantum computing at the University of Waterloo and a Canada Research Chair in Quantum Information.

APPENDIX D

Canada Research Chair in Quantum Information Processing

Université de Montréal
Natural Sciences and Engineering
514-343-6807

Gilles Brassard
brassard@iro.umontreal.ca

Research involves

The application of quantum mechanics to information processing

Computing Beyond the Speed of Light

In the first quarter of the 20th century, Albert Einstein revolutionized physics with the theory of quantum mechanics. At the beginning of the 21st century, Gilles Brassard is applying quantum mechanics to computers.

Brassard says Quantum information-processing concepts have the potential to create a revolution in computer science. A revolution that could be as spectacular and far-reaching as that created decades ago by the invention of the transistor.

In the late 1970s, he was one of the first researchers to apply the theoretical physics of quantum mechanics to the burgeoning field of computer science-at a time when the notion was thought of more as science fiction than science.

Brassard will continue his groundbreaking work to apply the "spooky action" of quantum mechanics to information processing. Quantum mechanics explains the behavior of the building blocks of all matter and energy, such as photons, electrons, and atoms. His research will further explore the potential to create quantum computers-capable of performing some calculations faster than a classical computer the size of the universe, at least in theory. This could have profound consequences for the security of transactions on the Internet, as needed for secure Electronic Commerce.

Another area of enormous potential is quantum cryptography, a field in which Brassard has been a pioneer since 1979. Along with his extensive group of international graduate students and postdoctoral fellows, Brassard will seek to determine the conditions under which this quantum-based information privacy system could be practically used, yet unconditionally secure.

In addition to this research, Brassard will continue his research into the fascinating world of quantum teleportation. This makes use of the most fascinating aspects of quantum mechanics to allow for the transmission of quantum information through a classical channel.