Quantum Computing

Ishita Ray
University Institute of Engineering and Technology
Panjab University
Chandigarh, India
rayria06@gmail.com

***Abstract*— Changing the model underlying information and computation from a classical mechanical to a quantum mechanical one yields faster algorithms, novel cryptographic mechanisms, and alternative methods of communication. Quantum algorithms can perform a select set of tasks vastly more efficiently than any classical algorithm, but for many tasks it has been proven that quantum algorithms provide no advantage. The breadth of quantum computing applications is still being explored. Major application areas include security and the many fields that would benefit from efficient quantum simulation. The quantum information processing viewpoint provides insight into classical algorithmic issues as well as a deeper understanding of entanglement and other non-classical aspects of quantum physics. This text describes some of the introductory aspects of quantum computing.**

Keywords*— *quantum, information processing, qubit, classical, protocol.

I. Introduction

In the last two decades of the twentieth century, researchers recognized that the standard model of computation placed unnecessary limits on computation. Our world is inherently quantum mechanical. By placing computation on a quantum mechanical foundation faster algorithms, novel cryptographic mechanisms, and alternative methods of communication have been found. Quantum information processing, a field that includes quantum computing, quantum cryptography, quantum communication, and quantum games, examines the implications of using a quantum mechanical model for information and its processing. Quantum information processing changes not only the physical processes used for computation and communication, but the very notions of information and computation themselves.

In quantum computers we exploit quantum effects to compute in ways that are faster or more efficient than, or even impossible, on conventional computers. Quantum computing does not provide efficient solutions to all problems. Nor does it provide a universal way of circumventing the slowing of Moore's law as fundamental limits to miniaturization are reached. Quantum computation enables certain problems to be solved efficiently; some problems which on a classical computer would take more than the age of the universe, a quantum computer could solve in a couple of days. But for other problems it has been proven that quantum computation cannot improve on classical methods, and for yet another class, that the improvement is small.

Quantum computing combines quantum mechanics, information theory, and aspects of computer science. The field is a relatively new one that promises secure data transfer, dramatic computing speed increases, and may take component miniaturisation to its fundamental limit.

II. Elements of Quantum Computing

A. Bits and Qubits

The state space of a physical system consists of all possible states of the system. Any quantum mechanical system that can be modelled by a two dimensional complex vector space can be viewed as a qubit. Such systems include photon polarization, electron spin, and a ground state and an excited state of an atom. A key difference between classical and quantum systems is the way in which component systems combine. The state of a classical system can be completely characterized by the state of each of its component pieces. A surprising and unintuitive aspect of quantum systems is that most states cannot be described in terms of the states of the system's components.

Such states are called entangled states. Another key property is quantum measurement. In spite of there being a continuum of possible states, any measurement of a system of qubits has only a discrete set of possible outcomes; for n qubits, there are at most 2n possible outcomes. After measurement, the system will be in one of the possible outcome states. Which outcome is obtained is probabilistic; outcomes closest to the measured state are most probable. Unless the state is already in one of the possible outcome states, measurement changes the state; it is not possible to reliably measure an unknown state without disturbing it. Just as each measurement has a discrete set of possible outcomes, any mechanism for copying quantum states can only correctly copy a discrete set of quantum states. For an n qubit system, the largest number of quantum states a copying mechanism can copy correctly is 2n. For any state there is a mechanism that can correctly copy it, but if the state is unknown, there is no way to determine which mechanism should be used. For this reason, it is impossible to copy reliably an unknown state, an aspect of quantum mechanics called the no cloning principle.

A qubit has two arbitrarily chosen distinguished states, labelled |0i and |1i, which are the possible outcomes of a single measurement. Every single qubit state can be represented as a linear combination, or superposition, of these two states. In quantum information processing, classical bit values of 0 and 1 are encoded in the distinguished states |0i and |1i. This encoding enables a direct comparison between bits and qubits: bits can only take on two values, 0 and 1, while qubits can take on any superposition of these values, a|0i+b|1i, where a and b are complex numbers such that |a|2+|b|2 = 1.

Any transformation of an n qubit system can be obtained by performing a sequence of one and two qubit operations. Most transformations cannot be performed efficiently in this manner. Figuring out an efficient sequence of quantum transformations that can solve a useful problem is the heart of quantum algorithm design.

B. Entangled States

Subatomic particles can be entangled, this means that they are connected, regardless of distance. Their effect on each other upon measurement is instantaneous. This can be useful for computational purposes. Measuring entangled states accounts for the correlations between them.

C. Quantum Circuits

If we take a quantum state, representing one or more qubits, and apply a sequence of unitary operators (quantum gates) the result is a quantum circuit. We now take a register and let gates act on qubits, in analogy to a conventional circuit.

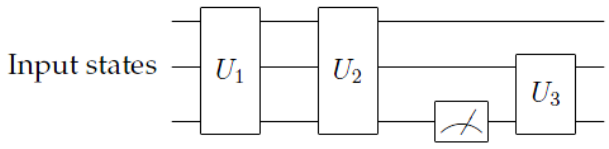

Figure 1. Simple Quantum Circuit

This circuit above is a series of operations and measurements on the state of *n*-qubits. Each operation is unitary and can be described by an 2*n* £ 2*n* matrix. Each of the lines is an abstract *wire*, the boxes containing *Un* are *quantum logic gates* (or a series of gates) and the meter symbol is a measurement. Together, the gates, wires, input, and output mechanisms implement quantum algorithms.

Unlike classical circuits which can contain loops, quantum circuits are “one shot circuits” that just run once from left to right (and are special purpose: i.e. we have a different circuit for each algorithm).

It should be noted that it is always possible to rearrange quantum circuits so that all the measurements are done at the end of the circuit. Quantum circuit diagrams have the following constraints which make them different from classical diagrams.

1. They are acyclic (no loops).

2. No FANIN, as FANIN implies that the circuit is NOT reversible, and therefore not unitary.

3. No FANOUT, as we can’t copy a qubit’s state during the computational phase because of the no-cloning theorem.

All of the above can be simulated with the use of ancilla and garbage bits if we assume that no qubits will be in a superposition. Garbage bits are useless qubits left over after computation and ancilla bits are extra qubits needed for temporary calculations.

The fundamental unit of quantum computation, the qubit, can take on a continuum of values, but a discrete version of quantum computation can be constructed that preserves the features of standard quantum computation.

III. Why Quantum Computing?

A. History

In 1982 Richard Feynman theorised that classic computation could be dramatically improved by quantum effects, building on this, David Deutsch developed the basis for quantum computing between 1984 and 1985. The next major breakthrough came in 1994 when Peter Shor described a method to factor large numbers in quantum poly-time (which breaks RSA encryption). This became known as Shor’s algorithm. At around the same time the quantum complexity classes were developed and the quantum Turing machine was described.

Then in 1996 Lov Grover developed a fast database search algorithm (known as Grover’s algorithm). The first prototypes of quantum computers were also Elements of Quantum Computing built in 1996. In 1997 quantum error correction techniques were developed at Bell labs and IBM. Physical implementations of quantum computers improved with a three qubit machine in 1999 and a seven qubit machine in 2000.

B. What classical computers can and cannot do

Computer scientists categorize problems according to how many computational steps it would take to solve a large example of the problem using the best algorithm known. The problems are grouped into broad, overlapping classes based on their difficulty. Three of the most important classes are listed below. Contrary to myth, quantum computers are not known to be able to solve efficiently the very hard class called NP-complete problems.

1) *P Problems*: Ones computers can solve efficiently, in polynomial time.

Example: Given a road map showing *n* towns, can you get from any town to every other town? For a large value of *n,* the number of steps a computer needs to solve this problem increases in proportion to *n*2, a polynomial. Because polynomials increase relatively slowly as *n* increases, computers can solve even very large P problems within a reasonable length of time.

2) *NP Problems*: Ones whose solutions are easy to verify.

Example: You know an *n*-digit number is the product of two large prime numbers, and you want to find those prime factors. If you are given the factors, you can verify that they

are the answer in polynomial time by multiplying them. Every P problem is also an NP problem, so the class NP contains the class P within it. The factoring problem is in NP but conjectured to be outside of P, because no known algorithm for a standard computer can solve it in only a polynomial number of steps. Instead the number of steps increases exponentially as *n* gets bigger.

3) *NP-complete problems*: An efficient solution to one would provide an efficient solution to all NP challenges. Example: Given a map, can you colour it using only three colours so that no neighbouring countries are the same colour? If you had an algorithm to solve this problem, you could adapt the algorithm to solve any other NP problem (such as the factoring problem above or determining if you can pack *n* boxes of various sizes into a trunk of a certain size) in about the same number of steps. In that sense, NP-complete problems are the hardest of the NP problems. No known algorithm can solve an NP-complete problem efficiently.

C. *Where quantum computing fits in*

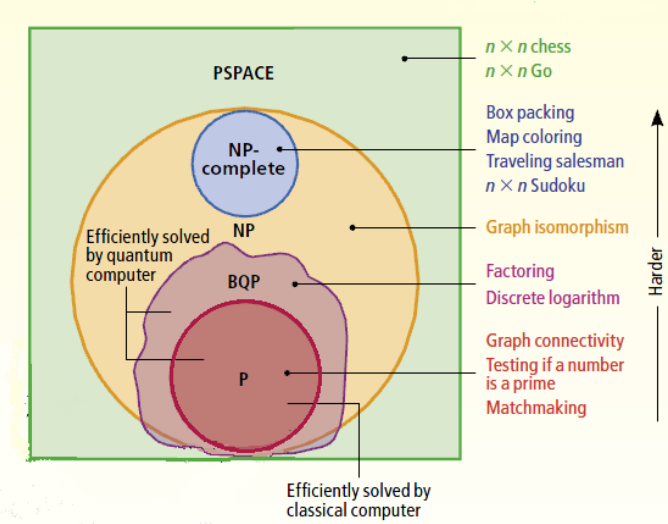

Figure 1. Various classes of computational problems

The map above depicts how the class of problems that quantum computers would solve efficiently (BQP) might relate to other fundamental classes of computational problems. (The irregular border signifies that BQP does not seem to fit neatly with the other classes.)

The BQP class (the letters stand for *b*ounded-error, *q*uantum, *p*olynomial time) includes all the P problems and also a few other NP problems, such as factoring and the so-called discrete logarithm problem. Most other NP and all NP-complete problems are believed to be outside BQP, meaning that even a quantum computer would require more than a polynomial number of steps to solve them.

In addition, BQP might protrude beyond NP, meaning that quantum computers could solve certain problems faster than classical computers could even check the answer. (Recall that a conventional computer can efficiently verify the answer of an NP problem but can efficiently solve only the P problems.) To date, however, no convincing example of such a problem is known.

Computer scientists do know that BQP cannot extend outside the class known as PSPACE, which also contains all the NP problems. PSPACE problems are those that a conventional computer can solve using only a polynomial amount of memory but possibly requiring an exponential number of steps.

IV. Implications and Applications

A. *Quantum Protocols*

Applications of quantum information processing include a number of communication and cryptographic protocols. The two most famous communication protocols are quantum teleportation and dense coding. Both use entanglement shared between the two parties that are communicating.

Quantum key distribution schemes were the first examples of quantum protocols. Quantum key distribution protocols establish a secret symmetric key between both parties, but their security rests on properties of quantum mechanics.

While "quantum cryptography" is often used as a synonym for "quantum key distribution," quantum approaches to a wide variety of other cryptographic tasks have been developed. Some of these protocols use quantum means to secure classical information. Others secure quantum information.

Many are "unconditionally" secure in that their security is based entirely on properties of quantum mechanics. Others are only quantum computationally secure in that their security depends on a problem being computationally intractable for a quantum computer.

Closely related to quantum key distribution schemes are protocols for unclonable encryption, a symmetric key encryption scheme that guarantees that an eavesdropper cannot copy an encrypted message without being detected. Unclonable encryption has strong ties with quantum authentication. One type of authentication is digital signatures. Quantum digital signature schemes have been developed, but the keys can be used only a limited number of times. In this respect they resemble classical schemes such as Merkle's one-time signature scheme.

B. *Broader Implications*

Quantum information theory has led to insights into fundamental aspects of quantum mechanics, particularly entanglement. Efforts to build quantum information processing devices have resulted in the creation of highly entangled states that have enabled deeper experimental exploration of quantum mechanics. These entangled states, and the improvements in quantum control, have been used in quantum microlithography to affect matter at scales below the wavelength limit and in quantum metrology to achieve extremely accurate sensors. Applications include clock accuracy beyond that of current atomic clocks, which are limited by the quantum noise of atoms, optical resolution beyond the wavelength limit, ultra-high resolution spectroscopy, and ultra-weak absorption spectroscopy.

The quantum information processing viewpoint has also provided a new way of viewing complexity issues in classical computer science, and has yielded novel classical algorithmic results and methods. Classical algorithmic results stemming from the insights of quantum information processing include lower bounds for problems involving locally decodable codes, local search, lattices, reversible circuits, and matrix rigidity. The usefulness of the complex perspective for evaluating real valued integrals is often used as an analogy to explain this phenomenon.

Cryptographic protocols usually rely on the empirical hardness of a problem for their security; it is rare to be able to prove complete, information theoretic security. When a cryptographic protocol is designed based on a new problem, the difficulty of the problem must be established before the security of the protocol can be understood. Empirical testing of a problem takes a long time. Instead, whenever possible, "reduction" proofs are given that show that if the new problem were solved it would imply a solution to a known hard problem.

C. Impact on security

Electronic commerce relies on secure public key encryption and digital signature schemes, as does secure electronic communication. Without secure public key encryption, authentication and the distribution of symmetric session keys become unwieldy.

Both factoring and the discrete logarithm problem are candidate NP intermediate problems. Hope for alternative public key encryption protocols centers on using other NP intermediate problems. The leading candidates are certain lattice based problems. Some of these schemes have impractically large keys, while for others their security remains in question. Also, Regev showed that lattice based problems are closely related to the dihedral hidden subgroup problem. The close relationship of the dihedral hidden subgroup problem with problems solved by Shor's algorithm makes many people nervous, though so far the dihedral hidden subgroup problem has resisted attack.

Given the historic difficulty of creating practical public key encryption systems based on problems other than factoring or discrete log, it is unclear which will come first, a large scale quantum computer or a practical public key encryption system secure against quantum and classical attacks. If the building of quantum computers wins the race, the security of electronic commerce and communication around the world will be compromised.

V. LIMITATIONS

Beals et al. proved that, for a broad class of problems, quantum computation cannot provide any speed-up. Their methods were used by others to provide lower bounds for other types of problems. Ambainis found another powerful method for establishing lower bounds. In 2002, Aaronson showed that quantum approaches could not be used to efficiently solve collision problems. This result means there is no generic quantum attack on cryptographic hash functions. Shor's algorithms break some cryptographic hash functions, and quantum attacks on others may still be discovered, but Aaronson's result says that any attack must use specific properties of the hash function under consideration.

Grover's search algorithm is optimal; it is not possible to search an unstructured list of N elements more rapidly than $O(\sqrt{N})$. This bound was known before Grover found his algorithm. Childs et al. showed that for ordered data, quantum computation can give no more that a constant factor improvement over optimal classical algorithms. Grigni et al. showed in 2001 that for most non-abelian groups and their subgroups, the standard Fourier sampling method, used by Shor and successors, yields exponentially little information about a hidden subgroup.

If a large, ideal quantum computer would face most of the same limitations as our present-day classical computers do, should the physicists working on the extraordinarily hard task of building even rudimentary quantum computers pack up and go home? The answer is no, for four reasons.

- If quantum computers ever become a reality, the "killer app" for them will most likely not be code breaking but rather something so obvious it is rarely even mentioned: simulating quantum physics. This is a fundamental problem for chemistry, nanotechnology and other fields, important enough that Nobel Prizes have been awarded even for partial progress.
- As transistors in microchips approach the atomic scale, ideas from quantum computing are likely to become relevant for classical computing as well.
- Quantum computing experiments focus attention directly on the most mystifying features of quantum mechanics—and hopefully, the less we can sweep those puzzles under the rug, the more we will be forced to understand them.
- Quantum computing can be seen as the most stringent test to which quantum mechanics itself has ever been subjected. In my opinion, the most exciting possible outcome of quantum computing research would be to discover a fundamental reason why quantum computers are *not* possible. Such a failure would overturn our current picture of the physical world, whereas success would merely confirm it.

VI. CONCLUSION

Will scalable quantum computers ever be built? Yes. Will quantum computers eventually replace desktop computers? No. Quantum computers will always be harder to build and maintain than classical computers, so they will not be used for the many tasks that classical computers do equally efficiently. Quantum computers will be useful for a number of specialized tasks. The extent of these tasks is still being explored.

However long it takes to build a scalable quantum computer and whatever the breadth of applications turns out to be,

quantum information processing has changed forever the way in which quantum physics is taught and understood. The quantum information processing view of quantum mechanics clarifies key aspects of quantum mechanics such as quantum measurement and entangled states. The practical consequences of this increased understanding of nature are hard to predict, but they can hardly fail to profoundly affect technological and intellectual developments in the coming decades.

REFERENCES

[1] Eleanor Rieffel, “Quantum Computing,” April 29, 2011.

[2] Riley T. Perry, “The Temple of Quantum Computing,” April 29, 2006.

[3] Scott Aaronson, “The Limits of Quantum,” *Scientific American*, p. 62-69, March 2008.

[4] Wikipedia-The free encyclopedia [Online]. Available: http://www.wikipedia.org/

[5] TheFreeDictionary.com [Online]- Available: http://encyclopedia.thefreedictionary.com/

[6] Wolfram, *A New Kind of Science*, 1st edition, Wolfram Media, USA, 2002.

[7] Science Blogs [Online]- Available: http://scienceblogs.com/

[8] R. Feynman. Feynman Lectures on Computation. Addison-Wesley, Reading, MA, 1996.