QUANTUM COMPUTERS: A PERSPECTIVE INTO NEXT GENERATION INFORMATION PROCESSING

Ipshita Chatterjee*

A quantum computer is a machine that utilizes quantum mechanical concepts for information processing, offering an exponential speedup and a considerable reduction in power consumption over conventional digital computers. The article discusses the properties of quantum computers and possibilities of their applications in different domains.

INTRODUCTION

Conventional digital computers use bits as fundamental units of computing. Instead, quantum computers exploit quantum mechanical properties for data storage and processing. Operations performed simultaneously on two bits can be performed on a single bit in a quantum computer, reducing memory and time required. This performance improves exponentially with increasing number of bits, indicating the superior information processing capability of quantum computers. However, any useful data stored in quantum bits is lost on interference with the external environment. This challenge has resisted the realization of a large scale commercial quantum computer till date.

HISTORY

Quantum properties were earlier believed to be the limit to reduction in computer size and their performance improvement. Richard Feynman[1], however, in May 1981, proposed the reevaluation of the basic laws of computing, to simulate quantum mechanics. Using the ideas of Fredkin and Toffoli[2], he further suggested a new system, called a quantum computer, which would possibly improve existing computing performance greatly. David Deutsch[3] followed this up further with a mathematical concept called the quantum Turing machine in 1985 to theoretically predict the feasibility of quantum computers. The works of Deutsch and Josza[4], and Bernstein and Vazirani during 1990s established the many advantages of quantum computers in finding solutions to problems, exponentially faster than conventional computers.

However, a pivotal development in the history of quantum computing was in 1994, when Peter Shor[5] developed a quantum algorithm which could factorize large integers (Table 1) and find discrete

Table 1 : Evolution of Integer Factorization Algorithms[7].

Algorithm	Running Time	Remarks
Trial Division	$O(\sqrt{N})$ bit operations	Inefficient classical algorithm
Pollard's ρ Algorithm	$O(N^{1/4}*(\log N)^2)$	Substantially faster for finding non- trivial factors
Quadratic Sieve	$O(e^{(1+\epsilon)\sqrt{(\log N \log\log N)}}),$ $\epsilon>0$	Fastest classical algorithm for integers under 100 decimal digits
General Number Field Sieve (GNFS)	$\exp((c+o(1))$ $(\log N)^{1/3}$ $((\log\log N)^{2/3}),$ $c \approx 1.526$	Fastest classical algorithm for all integer factorization
Shor's Algorithm	$O((\log N)^3)$	First quantum algorithm, exponential speedup over GNFS

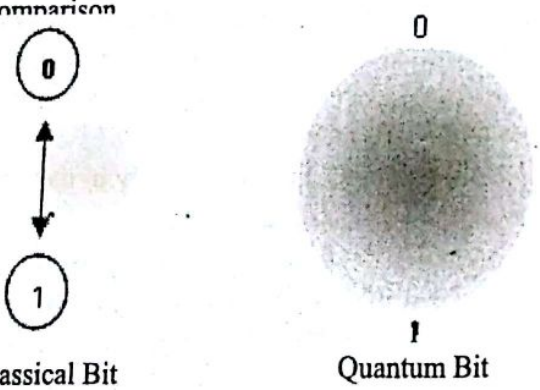
*Division of Computer Engineering, Netaji Subhas Institute of Technology, New Delhi 110078,E-mail:chatterjee08@gmail.com

logarithms, both of which are hard problems for digital computers to solve. This algorithm reduces the factoring problem to the classical problem of finding the group order and subsequently finding the period using quantum Fourier transform. Another algorithm for searching a value for a specified key in an unsorted database, a fundamental problem of computer science, was proposed by Grover[6] in 1996, which provided a quadratic speedup over the best possible conventional solution.

The development of quantum algorithms has given rise to another class of decision problems solvable by quantum computers in polynomial time, with a maximum error probability of 33%, known as bounded-error quantum polynomial time (BQP) problems. This class is the quantum analogue of the classical bounded-error probabilistic polynomial time (BPP) problems.

PROPERTIES OF QUANTUM COMPUTERS

The fundamental unit of computing in digital computers is a bit, an abbreviation for binary digit, which can exist in only two states, 0 and 1. Quantum computers have quantum bits or *qubits*, which can exist in 0, 1 and also as a superposition of 0 and 1 states. When existing in superposition, the qubit can be thought to be valued at 0 in one universe and 1 in another. Any operations on qubits operate on these two values at the same time. Fig.1 illustrates this comparison



Classical Bit Quantum Bit

Fig.1. Comparison of states of classical and quantum computers.

QUANTUM PARALLELISM

Four values can be simultaneously manipulated by operating on two qubits, eight values while operating on three qubits and so on. This property of parallel manipulation of multiple qubit values at the same time is known as *quantum parallelism*. Parallelism is the so-called magical element of quantum computers, the reason behind an exponential growth in the number of computations performed per unit time over that of a conventional computer.

QUANTUM SUPERPOSITION

The commonly used notation to denote qubits and their operations is the *Dirac notation*, or the *bra-ket notation*. Anything specified inside | > denotes a column vector. A single state of a qubit is represented as

$$\alpha|1> + \beta|0>$$

This is written as a linear combination of the states |1> and |0>, known as the basis states of the qubit. α and β are said to be the probabilistic amplitudes of the respective basis states. If a qubit is measured, then the answer will be 1 or 0 with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively. These probabilistic amplitudes sum to 1, implying that these are the orthonormal basis states for the given qubit. This property of qubits by which they exist as a linear combination of two basis states is known as *quantum superposition*. This coherent superposition continues to exist until there is no external interference in the system.

ENTANGLEMENT

The *entanglement* property of qubits is the basis of all quantum calculations. An entangled system is one in which the state of a single particle depends on those of all other particles. The state of the system is always expressed as a function of all the constituent states.

QUANTUM GATES

Any operation, called a *quantum gate*, performed on an entangled quantum system is reversible. Operand qubits are represented as column vectors and quantum gates as unitary matrices. Thus, the states of resultant qubits can be calculated through simple matrix multiplication. However, *measurement* of qubits is an irreversible operation and causes the entanglement of quantum states to

break. Thus, no intermediate measurement of quantum states is possible.

DECOHERENCE

The phenomenon where the entanglement of the system and all the computational data is destroyed is called *decoherence*, which prevents the physical realization of large scale quantum computers. The qubits must not have any physical interaction with the outside environment, as the superposition of states and quantum parallelism, exists only when the system is left isolated. Any interaction with the external surroundings, even with air molecules, can cause the entanglement of quantum states to collapse and leading to the loss of all useful data. The fragility of the system increases with the increase in the number of qubits.

QUANTUM COMPUTERS

Physical Realization: All simulations of quantum computers have only been performed on a small number of qubits so far. Presently, there exists no method of developing a quantum computer, suitable for commercial use, without the internal states becoming very fragile and collapsing. However, several technologies are being explored for physical realization of quantum computers.

Superconducting qubits are small electrical circuits which behave like artificial atoms. The discrete energy states of these atoms can be controlled by electrical excitations. So far, nine fully controllable qubits have been demonstrated through superconductivity. Quantum computers can also be realized through the trapped ion technology, where ions are suspended in free state using electromagnetic fields and qubits are stored in their stable electronic states. The fundamental quantum operations have been demonstrated with greatest accuracy in trapped ion systems.

APPLICATIONS

All possible applications of quantum computers are yet to be discovered. Currently it has been established that quantum computers provide many advantages over conventional computers and can potentially transform many domains of present-day technology. Some possible applications are discussed below.

1) Modern-day cryptosystems, which form the fundamentals of computer security, are based on the mathematical problems of integer factorization and discrete logarithms, and the inability of digital computers to solve them in a reasonable amount of time. Shor's algorithm showed that quantum computers will be able to decrypt many of these rapidly. Schemes like the public key based RSA scheme, used to secure WiFi, bank and email accounts, can easily be decoded by quantum computers. These computers will also be able to provide unbreakable security schemes, since any interception of intermediate quantum data destroys it completely and the source knows about the data breach.
2) Quantum computers provide a considerable advantage in problems of searching through huge amounts of data, which is crucial in the age of Big Data. Air travel could be further secured, by testing jet software which was too complex for digital computers. Distant planets could be discovered by processing large amounts of astronomical data and possibly, medicine could also be revolutionized by mapping entire genomes to create more effective therapies. Scientists could easily simulate quantum processes and chemical reactions to study behavior of particles and atoms under special and unusual conditions which are difficult to replicate physically.
3) Artificial intelligence is currently in its nascent stages and quantum computing might enable machines to become truly intelligent. Training artificial intelligence systems with the help of quantum computers will enable more accurate reflection of human thought processes and may even help develop something similar to intuition in machines. Such a training will be far more accurate than that carried out by conventional computers, due to minimum data losses and high data processing capabilities of quantum computers.

4) Quantum computing has a special significance in speeding up several key problems in machine learning and has led to the emergence of Quantum Machine Learning, for solving quantum information problems like linear systems of equations in polynomial time, clustering, pattern-matching and principal component analysis.
5) Quantum computation is fundamentally based on the computing paradigm of reversible logic, which is essential in designing low power VLSI circuits beyond the thermodynamic limits of computation.
6) The major disadvantage of classical super-computers is their huge power consumption. Tianhe 2, the world's fastest supercomputer consumes almost 17.6 MW. However, quantum computers with their quantum tunneling effect will reduce this by 100 times. Thus, quantum computers will outperform the fastest supercomputer in terms of speed, while actually reducing the power consumption.

Quantum Neural Networks – A Case Study

Artificial neural networks (ANN) are computational models which simulate the working of the human brain, for solving complex problems. Just like the brain, they consist of several layers of artificial neurons, each of which is connected to several others and can either enforce or inhibit the final output, depending upon predefined mathematical functions.

Quantum neural networks (QNN) are the next natural step in the evolution of neurocomputing systems, with some scientists believing that such networks will enable the modeling of brain functions like understanding, awareness and consciousness, along with providing massive information processing capabilities.

Ricks and Ventura[8] proposed a QNN model and its corresponding training method. The following QNN can be used to compute AND operation of two input registers.

Similar to ANN, there is an input layer, one or more hidden layers and an output layer, each of which is fully connected to the previous layer. Every node of the input layer is qubit register $|\alpha\rangle$. Each hidden layer, used for intermediate calculations denoted by $|\beta\rangle$, computes a weighted sum of the outputs of the previous layer. If this sum is above a certain threshold weight, which is input separately, then the node goes high, otherwise it remains low. The output layer checks accuracy of the computed value against the target value $|\Omega\rangle$. The QNN is trained with a set of input registers and a performance register maintained.

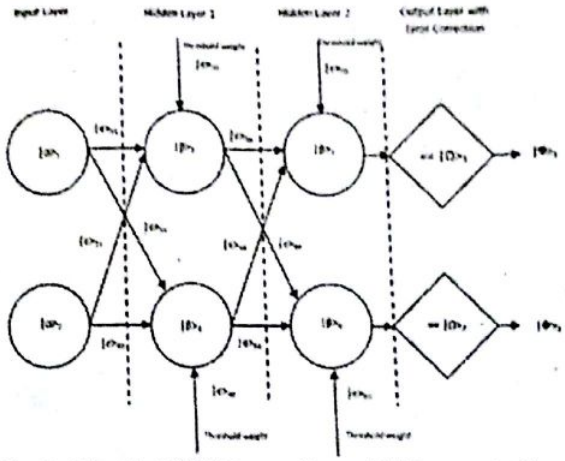


Fig.2. Simple QNN to perform AND opertation on two input qubit registers.

This is a small example of the power of quantum computing and its role in transforming artificial intelligence.

CONCLUSION

The possibilities of building and harnessing the power of quantum computers has gathered the interest of the entire technological community. Quantum computers could be the answers to many difficult problems, which otherwise could not be addressed by conventional computers at all, or could only be solved in very unrealistic amounts of time. It is expected that in the near future, R&D in algorithm design, artificial intelligence and quantum computing will make it possible to realize commercial scale quantum computers, which could solve several industrial and research problems, which remain unresolved due to the computational limitations of conventional computers.

ACKNOWLEDGEMENT

The author thanks Dr. Pinaki Chakraborty for reading a draft of this article and his constructive criticism.

REFERENCES

1) R. P. Feynman, *Int. J. Theor. Phys.*, **21**, 6, 467-488, 1982.
2) E. Fredkin and T. Toffoli, *Int. J. Theor. Phys.*, **21**, 219-253, 1982.
3) D. Deutsch, *P. Roy. Soc. Lond. A Mat.*, **400**, 97-117, 1985.
4) D. Deutsch and R. Josza, *P. Roy. Soc. Lond. A Mat.*, **1907**, 439-553, 1992.
5) P.W. Shor, *SIAM J. Sci. Comput.*, **26**, 1484-1506, 1997.
6) L. K. Grover, *Proceedings STOC*, 212-219, 1996.
7) K. Bimpikis and R. Jaiswal, *Univ. of California, San Diego*, pp. **1-15**, 2005.
8) B. Ricks and D. Ventura, *NIPS*, **16**, 1019-1026, 2003.