QUANTUM TECHNOLOGY AND ITS APPLICATIONS

Asst Prof. N Thrimooorthy¹, Brunda S²
¹Department of Master of Computer Applications, New Horizon College of Engineering
²Master of Computer Application, New Horizon College of Engineering

Abstract: Quantum computing is an emerging technology. The clock frequency of current computer processor systems may reach about 40 GHz within the next 10 years. By then, one atom may represent one bit. Electrons under such conditions are no longer described by classical physics, and a new model of the computer may be necessary by that time. The quantum computer is one proposal that may have merit in dealing with the problems presented. Currently, there exist some algorithms utilizing the advantage of quantum computers. For example, Shor’s algorithm performs factoring of a large integer in polynomial time, whereas classical factoring algorithms can do it in exponential time. In this paper we briefly survey the current status of quantum computers, quantum computer systems, and quantum simulators.

Keywords: Classical computers, quantum computers, quantum computer systems, quantum simulators, Shor’s algorithm.

I. INTRODUCTION

How much can the performance of a computer be improved? According to Moore’s law, if the performance keeps improving by means of technological innovations, which has occurred over the last few decades, the number of transistors per chip may be doubled every 18 months. Furthermore, processor clock frequency could reach as much as 40 GHz within 10 years [1]. By then, one atom may represent one bit [1]. One of the possible problems may be that, because electrons are not described by classical physics but by quantum mechanics, quantum mechanical phenomenon may cause “tunneling” to occur on a chip. In such cases, electrons could leak from circuits. Taking into account the quantum mechanical characteristics of the one-atom-permit level, quantum computers have been proposed as one way to effectively deal with this predicament. In this way, quantum computers can be used to solve certain computationally intense problems where classical computers require large amounts of processing time. Notwithstanding, further improvements will be necessary to ensure quantum computers’ proper performance in future, but such improvements seem obtainable. Currently, there exist some algorithms utilizing the advantage of quantum computers. For instance, the polynomial-time algorithm for factoring a large integer with O(n³) time was proposed by Peter Shor. This algorithm performs factoring exponentially faster than classical computers. This algorithm could factor a 512-bit product in about 3.5 hours with 1 GHz clock rate [3], whereas the number field sieve could factor the same product in 8400 MIPS years (One MIPS year is the number of instructions that a processor can execute in a year, at the rate of millions of instructions per second.) Another famous quantum algorithm is a database search algorithm proposed by Lov Grover that will find a single item from an unsorted list of N elements with O(√N) time. In this paper we briefly survey quantum computers. First, the main characteristics of quantum computers, superposition states, and interference are introduced. Then, current approaches to quantum computers are reviewed. Next, research on quantum computer simulators is introduced. We conclude with a few remarks.
II. QUANTUM COMPUTER SYSTEMS

1. Superposition State:
In classical computers, electrical signals such as voltages represent the 0 and 1 states as one-bit information. Two bits indicate four states 00, 01, 10, and 11, and n bits can represent 2^n states. In the quantum computer, a quantum bit called “qubit,” which is a two-state system, represents the one-bit information. For instance, instead of an electrical signal in classical computers, an electron can be used as a qubit. The spin-up and spin-down of an electron represent two states: 0 and 1, respectively. A photon can also be used as a qubit, and the horizontal and vertical polarization of a photon can be used to represent both states.

2. Literature survey of quantum computer
The first and second quantum revolutions: There are many devices available today which are fundamentally reliant on the effects of quantum mechanics. These include: laser systems, transistors and semi-conductor devices and other devices, such as MRI imagers. These devices are often referred to belonging to the 'first quantum revolution'; the UK Defense Science and Technology Laboratory (Dstl) grouped these devices as 'quantum 1.0',[6] that is devices which rely on the effects of quantum mechanics. Quantum technologies are often described as the 'second quantum revolution' or 'quantum 2.0'. These are generally regarded as a class of device that actively create, manipulate and read out quantum states of matter, often using the quantum effects of superposition and entanglement.

2.1. History:
The field of quantum technology was first outlined in a 1997 book by Gerard J. Milburn,[7] which was then followed by a 2003 article by Jonathan P. Dowling and Gerard J. Milburn,[8][9] as well as a 2003 article by David Deutsch.[10] The field of quantum technology has benefited immensely from the influx of new ideas from the field of quantum information processing, particularly quantum computing. Disparate areas of quantum physics, such as quantum optics, atom optics, quantum electronics, and quantum nanomechanical devices, have been unified under the search for a quantum computer and given a common language, that of quantum information theory.

The Quantum Manifesto was signed by 3,400 scientists and officially released at the 2016 Quantum Europe Conference, calling for a quantum technology initiative to coordinate between academia and industry, to move quantum technologies from the laboratory to industry, and to educate quantum technology professionals in a combination of science, engineering, and business.[11][12][13][14][15]

The European Commission responded to that manifesto with the Quantum Technology Flagship, a €1 Billion, 10-year-long megaproject, similar in size to earlier European Future and Emerging Technologies Flagship projects such as the Graphene Flagship and Human Brain Project.

III. APPLICATION FOR QUANTUM COMPUTING.
3.1. Machine Learning: Machine learning is a hot area right now because we are now seeing significant deployments at the consumer level of many different platforms. We are now seeing aspects of this every day in voice, image and handwriting recognition, to name just a few Examples. But it is also a difficult and computationally expensive task, particularly if you want to achieve good accuracy. Because of the potential payoff, there is a lot of research ongoing based upon sampling of Boltzmann distributions.
3.2. Computational Chemistry: There are many problems in materials science that can achieve a huge payoff if we just find the right catalyst or process to develop a new material, or an existing material more efficiently. There is already a significant effort in using classical computers to simulate chemical interactions, but in many cases the problems become Intractable for solving classically. So the original idea presented by Richard Feynman is why not use a quantum computer to simulate the quantum mechanical processes that occur.

3.3. Logistics and Scheduling: Many common optimizations used in industry can be classified under logistics and scheduling. Think of the airline logistics manager who needs to figure out how to stage his airplanes for the best service at the lowest cost. Or the factory manager who has an ever changing mix of machines, inventory, production orders, and people and needs to minimize cost, throughput times and maximize output. Or the pricing manager at an automobile company who needs to figure out the optimum prices of all the dozens car options to maximize customer satisfaction and profit. Although, classical computing is used heavily to do these tasks, some of them may be too complicated for a classical computing solution whereas a quantum approach may be able to do it.

3.4. Drug Design: Although drug design is really a problem in computational chemistry, I put it into its own classification because it is used by the pharmaceutical industry. Many of the drugs being developed still do so through the trial and error method. This is very expensive and if more effective ways of simulating how a drug will react would save a ton of money and time.

3.5. Cyber Security: Cyber security is becoming a larger issue every day as threats around the world are increasing their capabilities and we become more vulnerable as we increase our dependence upon digital system. Various techniques to combat cyber security threats can be developed using some of the quantum machine learning approaches mentioned above to recognize the threats earlier and mitigate the damage that they may do.

IV. OPEN CHALLENGE OF QUANTUM COMPUTERS

4.1. What is the threshold for universal quantum computing?
I mean this in both a narrow and a broad sense. The narrow sense: what is the maximum probability of decoherence per qubit per time step under which universal quantum computing is still possible? This is arguably the central question facing quantum computer builders, and it's entirely theoretical in nature.

4.2. The flip side:
what quantum systems can be simulated in classical polynomial time? Though we don't always appreciate it, this is a question of direct and immediate interest to condensed-matter physicists (or so they tell me!). We know basically three examples with nontrivial classical simulations: stabilizer circuits, fermionic systems with noninteracting modes, and quantum computers with bounded Schmidt rank (a measure of entanglement). Are there common generalizations of these three examples? Also, can we efficiently simulate a quantum computer that's (say) always in a separable mixed state, or always in a state represent able by a small number of linear combinations and tensor products?

4.3. BQP versus classical complexity classes.: After twelve years of effort, not only do we still not know whether BQP sits in the classical polynomial hierarchy, there's really no evidence either way. There's an oracle relative to which BQP is not in MA, but we still have no oracle
relative to which BQP is not in AM. At least in the unrelativized world, I consider it entirely possible that BQP is contained in AM intersect coAM (and thus in NP intersect coNP under a derandomization assumption). This would mean that whenever a quantum computer yields a particular outcome, there's a short classical proof that it does so.

4.4. The power of small-depth quantum circuits.
Is BQP = BPPBQNC? In other words, can the "quantum" part of any quantum algorithm be compressed to polylog(n) depth, provided we're willing to do polynomial-time classical postprocessing? (This is known to be true for Shor's algorithm.) If so, building a general-purpose quantum computer would be much easier than is generally believed! Incidentally, it's not hard to give an oracle separation between BQP and BPPBQNC, but the question is whether there's any concrete function "instantiating" such an oracle.

4.5. Quantum learning.
Can the concept class of AC0 circuits be PAC-learned in quantum polynomial time? (The best known classical algorithm takes nlog n time.) More audaciously, can the concept class of TC0 circuits be PAC-learned in quantum polynomial time? If so, then quantum computers would have an enormous advantage over classical computers in learning close-to-optimal weights for neural networks. In my view, there are two facts that make this a serious possibility: first, that the best classical learning algorithms so often work by learning the Fourier spectrum of the function of interest. And second, that the only evidence that learning TC0 circuits is hard classically comes from the presumed intractability of the factoring and discrete log problems.

V. TOOLS OF QUANTUM COMPUTER

5.1. Microsoft Quantum Development Kit:
Microsoft has released a preview version of their Quantum Development Kit that appears to supersede their earlier LIQUi|> software. This kit features a newly named quantum programming language called Q#, integration with their Visual Studio development environment, simulators that run on either a local system or their powerful Azure cloud platform, and rich libraries and code samples that can be used as building blocks. IBM Quantum Experience: IBM has put an experimental 5 qubit gate-level quantum processor on the web and is allowing members of the public to apply to get access to it. At the IBM Quantum Experience website there are four modules; a short tutorial that explains the basics of quantum computation and instructions on how to use it, a quantum composer that allows one to configure quantum gates for the qubits, a simulator which allows one to simulate their configuration before running it on the actual machine, and finally access to the machine itself which allows one to run their configuration and view the results. Rigetti Forest: The Rigetti Forest suite consists of a quantum instruction language called Quil, an open source Python library for construction Quil programs called pyQuil, a library of quantum programs called Grove, and a simulation environment called QVM standing for Quantum Virtual Machine. pyQuil and Grove are open source programs available on Github. Users would develop their programs using pyQuil and Grove on their own computer and then submit them to QVM for simulation over a web portal that is available for registered users. ProjectQ: ProjectQ is an open-source software framework for quantum computing implemented in Python. It allows users to implement their quantum programs in Python using a powerful and intuitive syntax. ProjectQ can then translate these programs to any type of back-end, be it a simulator run on a classical computer or an actual quantum chip including the IBM Quantum Experience platform. Other hardware platforms will be supported in the future.
VI. CONCLUSION
In this paper we have reviewed the principles, algorithms, and hardware considerations for quantum computing. Several research groups are investigating qubits and quantum logic circuitry using different resources (i.e., atom, ion, electron, and photon, among others). The realization of a practical quantum computer is expected before we encounter the limit of Moore’s law with respect to imp movements that may be possible using the classical computer model. A current realizable quantum computer is based on seven-bit NMR, which can factor 15. Further research is needed, for example, via simulation, on quantum computers using classical computers. Such a simulator must be able to handle quantum computers that operate on a practically large number of qubits. To this end, we need to employ large-scale parallel processing methods to acquire more meaningful results within a practical time frame. By applying the methods/concepts of classical computers such as hardware abstraction to quantum computers, the research progress may be accelerated. For example, some groups proposed quantum programming languages that allow us to think of quantum computer operations in an abstract manner as we do with a classical computer[16–17]. Efforts at realization for quantum computers have just begun. Undoubtedly, we need more intensive research in a physical realization of components of quantum computers [18]. Computer scientists/engineers will need to consider the various architectural solutions for quantum computers as well as the various new (practical) quantum algorithms to advance the state of the art for quantum computers.

REFERENCES
I. C.P. Williams & S.H. Clearwater, Exploration in quantum computing (New York: Springer-Verlag, 1997).
II. P.W. Shor, Algorithm for quantum computation: Discrete logarithm and factoring, Proc. 35th IEEE Annual Symp. On Foundations of Computer Science, Santa Fe, NM, November 1994, 24–134.
III. M. Oskin, F.T. Chong, & I. Chuang, A practical architecture for reliable quantum computers, IEEE Computer, January 2002, 79–87.
IV. B. Preneel (Ed.), Factorization of a 512-bit RSA modules, Lecture Notes in Computer Science, Vol. 1807 (Berlin: Springer-Verlag, 2000).
V. L.K. Grover, A fast quantum mechanical algorithm for database search, Proc. STOC, Philadelphia, 1996, 212–219.
VI. https://www.epsrc.ac.uk/newsevents/pubs/dstl-uk-quantum-technology-landscape-2014/]
VII. Schrödinger's Machines, G.J.Milburn, W H Freeman & Co. (1997) Archived August 30, 2007, at the Wayback Machine.
VIII. "Quantum Technology: The Second Quantum Revolution," J.P.Dowling and G.J.Milburn, Phil. Trans. R. Soc. A 361, 3655 (2003)
IX. "Quantum Technology: The Second Quantum Revolution," J.P.Dowling and G.J.Milburn, arXiv:quant-ph/0206091v1
X. "Physics, Philosophy, and Quantum Technology," D.Deutsch in the Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing, Shapiro, J.H. and Hirota, O., Eds. (Rinton Press, Princeton, NJ. 2003) “QuantumManifestoforQuantumTechnologies” "Quantum Manifesto”
XI. lexander Hellemans. Europe Bets €1 Billion on Quantum Tech: A 10-year-long megaproject will go beyond quantum computing and cryptography to advance other emerging technologies”. July 2016.
XII. IEEE Spectrum. Michael Allen. "Quantum manifesto’ for Europe calls for €1bn in funding”. 2016. Physics World. "Quantum Manifesto: Europe Leads in Quantum Technology”. 2016.
XIII. J. Niwa, K. Matsumoto, & H. Imai, General-purpose parallel simulator for quantum computing, Physical Review A, 66, 2002, 062317-1–062317-11.
XIV. J.W. Sanders & P. Zuliani, Quantum programming, Mathematics of program construction, Lecture Notes in Computer Science, 1837 (Heidelberg: Springer Verlag, 2000), 80–99.
XV. B. Omer," Classical concepts in quantum programming, Quantum Structures,2002, http://arxiv.org/abs/quant-ph/0211100.
XVI. P. Selinger, Towards a quantum programming language, Mathematical Structures in Computer Science, 14, 2003, 527.