International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

QUANTUM COMPUTING'S HIGH PERFORMANCE

Tamanna Punia[1], Attar Singh[2]

[1]*Arya College of Education Hisar, CRS Univ. Jind (Haryana) India*

[2]*Assoc. Prof. HOD Physics, CRM PG College, Hisar (Haryana) India*

ABSTRACT

Altering the model underlying information and computation from a classical mechanical to a quantum mechanical gives faster algorithms. The architecture scalability afforded by recent proposals of a large-scale photonic-based quantum computer allows us to move on to a discussion of massively scaled Quantum Information Processing (QIP). Some of the proposed activities call for a dialogue between the quantum computing (QC) community and high-performance computing (HPC) community. In this paper, we consider the quantum analogue of High Performance Computing (HPC), in which a dedicated server farm is used by several users to run algorithms and share quantum data. HPC has increasingly contributed to diverse scientific fields, ranging from materials science to biology and biomedicine, including genomics and neuroscience.

Keywords: Quantum computing, High Performance Computing, secure computing, topological clusters

I. INTRODUCTION

The computer technology has evolved from gears to relays to valves to transistors to integrated circuits and so on. Due to the presence of advanced lithographic techniques, one can compress fraction of large micron login gates and wires onto the surface of silicon chips which results into even smaller parts and assured to reach a stage where logic gates are so little that are made out of only handful of atoms. The rules of quantum mechanics are obeyed by the matter at atomic scale and such rule varies from the classical rules which determine the various properties of ordinary logic gates. So, new quantum technology must supplement present technology in order to have smaller computers in the future. Based on quantum principles, quantum computers can support completely new type of computation with qualitatively new algorithms.

A quantum computer makes straight use of quantum mechanical phenomena such as superposition and entanglement, (it is the ability for pairs particles to interact over any distance) for carrying out operations on data. Both quantum and digital computers vary from each other. The basic idea behind digital computers is the use of transistors in them which needs data to be encoded in form of binary digits (bits) while in quantum computation to represent data and to perform operations on such data quantum properties are used. It is expected that in the coming 8 years that is in around 2025, transistors and chips will be no longer present in computers. When we think of computers first thing that comes to our mind is the common classical silicon computer (digital computer). Every one of us thinks that these are the fastest. But, quantum computes are faster than classical ones. Quantum computers are a next general of classical computers according to scientists. The technology used in quantum computers is very much different from classical ones. Quantum computer uses bits of quantum (qubits) for operation. The nature of Qubit is quaternary. The laws of quantum mechanics are totally different from classical mechanics. The main difference between bit and qubit is that qubit can not only exist in 0 or 1 logical values, but also in linear combination of 0 and 1 state due to the phenomenon of principle of superposition of quantum mechanics. The superposition state is one in which a qubit can be both 0 and 1 simultaneously. Eight qubits are combined to form a qubyte which is similar to a byte of a classical computer but qubyte can have all values from 0 to 255 simultaneously unlike a byte which can’t take all values simultaneously due to the lack of presence of superposition principle.

In classical computers, calculations are performed significantly in the same way as by hand. Consequently, the class of problems that can be solved efficiently is the same as the class that can be solved efficiently by hand. Here “efficiently”, refers to the idea that the evaluation time doesn’t grow too quickly with the size of the input. While in quantum computers, calculations are done by unitary transformations on the state of quantum bits. Combines with the principle of superposition, this creates possibilities that are not available for hand calculations. This translates into more efficient algorithms for a.o. factoring, searching and simulation of quantum mechanical systems. First 16- bit quantum computers were build by IBM Q industry . Along with the IBM computer a company known as D-Wave has also been developing their own version of a quantum computer which is based on a process called annealing.

Since the introduction of quantum information science, a large scale physical device capable of high accuracy quantum information processing (QIP) has been a significant and highly desired after goal. While quantum information has lead to many remarkable developments in foundational quantum theory, solid state physics, quantum atom/optics and optics many researchers, worldwide, are still struggling towards making a large scale, quantum computer.

It has been an intensive area of research for not only physicists but also computer scientists, mathematicians and network analysts regarding the issue of computational scalability for QIP and in the last decade there have been many proposals for scalable quantum devices for a variety of quantum architectures[1]-[9]. In designing a large scale quantum computer the complexity involved is immense and research in this field must include complex ideas in experimental and theoretical physics, quantum error correction, network design, information theory and quantum algorithms. It has been difficult to execute theoretically scalable ideas in quantum information theory, error correction and algorithm design due to the relative beginnings of theoretical and experimental QIP into an architectural model where the transition from 1-100 qubits to 1-100 million qubits is conceptually straight-forward.

An extremely elegant pathway to realize an exceedingly large QIP system in optics has been introduced by the recent theoretical advancements in computational models for QIP. An extremely promising computational model for QIP known as Topological cluster state computing has been first introduced by Raussendorf, Harrington and Goyal [10]-[12]. Optical realization of quantum computer has been achieved by combining this model with chip based photon/photon gates such as the photonic module [13]. For the first time, the conceptual scalability of the chip based topological computer allows a grounded discussion on large scale quantum information processing, beyond the individual computer. In this paper we consider one step further the scalability issue, observing the possible long term applicability of topological cluster state computing with the photonic chip and discuss the future aspects of this architectural model of QIP.

II. HIGH PERFORMANCE QUANTUM COMPUTING (HPQC)

In the case of the optical topological computer[5] we can consider the possibility of mainframe computer and initiate to consider the quantum analogue of classical high performance computing, namely High Performance Quantum Computing (HPQC) in which a big, generic quantum resource is made available to multiple clients to perform joint (or joint) QIP. For various reasons, the topological computer is specially suited to this task. Apart from the resource benefits and error correcting of the topological cluster model, the fundamental geometric structure of the lattice allows for multi-user computation that would be problematic when using the more traditional 2D cluster state techniques [14]. While traditional computers the scalability in QIP is generally limited to the issue of making a single, moderately large scale quantum computer which is capable of performing significant algorithms for a single user. In traditional 2D cluster state computing, one dimension of the cluster signifies stimulated time. Since one dimension of the two is stimulated time, the algorithmic qubits arrangement forms an effective Linear Nearest Neighbour (LNN) network. Therefore, if multiple users are sharing a common 2D cluster state, the users could not interact data with each other oe with a central resource core without transferring quantum information through parts of cluster dedicated to other users.

In topological clusters, first LNN network topology is converted into 2D grid, enabling the partitioning of the cluster lattice into resource regions and user regions. We can potentially combine a mainframe model with developments in entanglement distribution and quantum communication [15]-[17]. This gives a layer of security to the HPQC which would be difficult, if not possible to achieve for multi-user, matter based qubit architectures. Here we discuss two possible mainframe models, one where partitions of the mainframe lattice are sent via quantum communications channels to individual users and the other where multi-user computation is performed locally by the mainframe. We give a basic estimate of the number of photonic chips used for a massive quantum server and hence complete the discussion by giving an example of a partition structure for the mainframe lattice which satisfies many of the important components for a HPQC.

The second model we consider here is named as trusted mainframe model. This is the place where individual users connect via classically safe data pathways and the mainframe host is trustworthy. Corresponding to the desired quantum algorithm, each client logs onto the host and transfers a classical data stream to the host (via sequence of photon measurement bases). Then the quantum algorithm is run by the mainframe locally and once the computation is done, transmits the resulting classical information back to the user. This model has very meaningful benefits. First, all that is required is that each user compiles a quantum algorithm into a suitable classical data stream which is sent to the mainframe since each user does not require quantum communication channels or any quantum infrastructure locally. During computation, there is no need to transfer any data by the host to the user. Internal corrections which arise due to lattice preparation and error correction procedures are done within the mainframe. The classical result from the quantum algorithm is the only data which is transmitted to the user. In the last, to run the quantum algorithm each user independently logs on to the system, the mainframe can be configured to allocate resources dynamically. If the mainframe load is low and one user needs a large number of logical qubits, then the host can adjust to assign a larger partition of the complete lattice to one individual user.

For high performance computing, the mainframe/user interaction of this model is similar to classical models. The possibility of secure HPQC is due to the fact that we are working with qubits. If sensitive computation is needed, we can integrate the mainframe with high exactness communication channels to do a secure version of HPQC in a manner which is not available to classical distributed computing.

We are able to utilize high accuracy optical communications channels to physically transmit a part of the 3D lattice to the client since the topological lattice is prepared by the mainframe is photon based. If we compare with the trusted mainframe model, there are some technological disadvantages of this scheme. For faithful transmission of entangled photon from mainframe to each client, high fidelity quantum communication channels are needed. Secondly, each client must have access to a specific amount of quantum technology, certainly, a set of classically controlled, high accurate single photon, detectors and wave- plates. This allows each client to perform their own measurement of the photon stream to perform computation locally.

As the quantum data stream never carries information related to the quantum algorithm being run on the client side hence security arises. It is the 3D topological lattice generated by the mainframe when photon stream is transmitted to the client, as the state transmitted is universally known, interrogation of the quantum channel is unnecessary. No other classical data is ever transmitted to or from the user except the starting eigenvalues of the prepared lattice (obtained from the mainframe preparation network), the only classical information and data sent between user and mainframe which indicates that an eavesdropper will not be able to know the basis the user chooses to measure in or have access to the classical error correction record even if they successfully taps into the quantum channel and entangles their own qubits to the cluster. So, without the access to the classical information record measurement by the client the ability to extract useful information from the quantum channel is impossible.

In addition to such benefits, the other benefit to the secure model is that the ultimate control of whether the portion of the lattice generated by the host remains entangled with the larger global lattice of the mainframe lies in the hands of the client. One can simply disentangles photon from the lattice by performing σ_z basis measurements on any photon within the cluster. Therefore, when partial segment of the generated lattice to the client is transmitted by the mainframe, they simply do σ_z basis measurements on photons around the edge of their partitioned allotment and neither the host and/or other users sharing the mainframe lattice can interact their portion of the lattice with the allotted section of the clients, it is guaranteed. It is generally recommended this slicing of the users sub lattice from the mainframe otherwise error correction procedures would need to be coordinated with the mainframe and classical data continually exchanged due the ability of the error chains to bridge the region between host and user when links remain impaired.

The option is provided to the users when they completed their task which is they can make their results available to the global lattice, either to be shared with other users or to be utilized again. Clients can measure all defect qubits and restore their part of the lattice to a defect free state if they do not wish to share the final quantum state of their algorithm. Once the quantum algorithm is completed clients can cease to measure the photons on the boundary of their allotted lattice if they wish to make available a non- trivial quantum state to the mainframe. Once the system is logged off by the client, the quantum state of the defect qubits within this lattice will remain (provided to enact identity operations the mainframe automatically continuously measures the sub- lattice). As a result, at a further time, it is the decision of the original user to log onto the system again, or another user may choose to log on the sliced sub-lattice and continue to change the stored data as they see fit (here the assumption is that to allow for significant error protection and hence long term storage, global lattice is of sufficient size).

Therefore, to allow different users to interact quantum states, this same methodology can be utilized. It is the decision of the two users to perform private, independent, quantum algorithms up to some limited time and then interact data (as done in the previous case). In the end, it is the duty of each user to cease severing the connections to the global lattice and then mainframe sends half an encoded Bell state, allowing for the implementation of teleportation protocols.

III. CONCLUSION

In High Performance Quantum Computer a massive 3- dimensional cluster lattice is used as a non- specific resource for multiple-user quantum information processing. For the conceptual scaling of a large topological cluster mainframe the architectural model of 3D topological clusters in optics is used, well beyond what could theoretically be done with other architectures for QIP. An illustration is given in which a possible lattice partitioning of the mainframe system. Although these partitions are not optimal but shows some of the most important structures that would be needed for multi-user quantum computing. An estimate of the number of photonic chips required to construct a mainframe device is calculated with the help of this partition structures. Approximately 7.5 billion photonic chips when constructed leads to a remarkably large multi-user quantum computer. This sized computer would represent the final goal of QIP research that began in late 1970's, although this is certainly a difficult task.

REFERENCES

[1] D. Kielpinski, C. Monroe, and D.J. Wineland, "Architecture for a large-scale ion-trap quantum computer", *Nature*, vo.417, pp.709-711, 2002.

[2] J.M.Taylor et. al., "Fault-tolerant architecture for quantum computation using electrically semiconductor spins," *Nature Phys*., vol.1, pp. 177-183, 2005.

[3] L.C.L. Hollenberg, A.D. Greentree, A.G. Fowler, and C.J. Wellard, " Two-dimensional architectures for donor-based quantum computing," *Phys. Rev.B*, vol.74, 045311, 2006.

[4] A.G.Fowler et. al., "Long-range coupling and scalable architecture for superconducting flux qubits," *Phys. Rev.B,* vol.76, 174507, 2007.

[5] S.J. Devitt et. al., "Architectural design for a topological cluster state quantum computer," *New. J. Phys.*, vol.11, 083032, 2009.

[6] R.Stock and D.F.V. James, "Scalable, High-Speed Measurement-Based Quantum Computer Using Trapped Ions," *Phys. Rev.Lett*., vol.102, 170501, 2009.

[7] R.van Meter, T.D. Ladd, A.G. Fowler, and Y. Yamamoto, "Distributed Quantum Computer Architecture Using Semiconductor Nanophotonics," *Int. J. Quant. Info*., vol.8, pp. 295-323,2010.

[8] D.A. Herrera-Marti, A.G. Fowler, D. Jennings, and T. Rudolph, "Photonic implementation for the Topological cluster-state quantum computer," *Phys. Rev.A.*, vol.82, 032332, 2010.

[9] N. Cody Jones et. al., "A Layered Architecture for Quantum Computing Using Quantum Dots," arXiv: 1010.5022,2010.

[10] R. Raussendorf and J. Harrington, “Fault-Tolerant Quantum Computation with High Threshold in Two Dimensions,” *Phys. Rev.Lett.*, vol.98, 190504, 2007.

[11] R. Raussendorf and J. Harrington, and K. Goyal, “Topological fault-tolerance in cluster state quantum computation,” *New. J. Phys.*, vol.9, p.199, 2007.

[12] A.G. Fowler and K. Goyal, “ Topological cluster state quantum computing”, *Quant. Inf. Comp.*, vol.9, no.9 & 10, pp.721-738,2009.

[13] S.J. Devitt et. al., “Photonic module: An on-demand resource for photonic entanglement,” *Phys. Rev.A.*, vol.76, 052312, 2007.

[14] R. Raussendorf and H.J. Briegel, ”A One-Way Quantum Computer,” *Phys. Rev.Lett.,* vol.86,p. 5188, 2001.

[15] P. Villoresi et. al. “Experimental verification of the feasibility of a quantum channel between space and Earth,” *New. J. Phys.*, vol.10, 033038, 2008.

[16] R. Ursin et. al. Proc. 2008 *Microgravity Sciences and Process Symposium* (2008); SECOQC, Project www.sqcoqc.net.

[17] W.J. Munro et. al., “From quantum multiplexing to high-performance quantum networking,” *Nature Photonics*, vol.4, pp.792-796,2010.

[18] A. Barenco, D. Deutsch, A. Ekert and R. Jozsa, Phys. Rev. Lett. 74, 4083 (1995).

[19] A. Kitaev and J. Watrous. Parallelization, ampli_cation, and exponential time simulation of quantum interactive proof systems. In Proceedings of the 32nd ACM Symposium on the Theory of Computing, pages 608{617. ACM, New York, 2000.

[20] A. Kitaev. Quantum computations: Algorithms and error correction. Russian Mathematical Surveys, 52(6), 1997.

[21] Archil Avaliani (2002)” Quantum Computers” International University.

[22] Biham, E., et al. (2004), ‘Quantum computing without entanglement’, Theoretical Computer Science, 320: 15–33.

[23] Bub, J. (2005), ‘Quantum mechanics is about quantum information’, Foundations of Physics, 34: 541–560.

[24] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. SIAM Journal on Computing, 26(5):1510{1523, 1997.

[25] C. Bennett, G. Brassard, and A. Ekert. Quantum cryptography. Scienti_c American, pages 50{57, October 1992.

[26] C. Bennett. Logical reversibility of computation. IBM Journal of Research and Development, 17(6):525{532, November 1973.

[27] C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano and D.J. Wineland, Phys. Rev. Lett. 75, 4714 (1995).

[28] Cirac, J.I. and Zoller, P. (1995), ‘Quantum computations with cold trapped ions’, Phys. Rev. Lett., 74: 4091–4094.

[29] D. Boneh and R. Lipton. Quantum cryptanalysis of hidden linear functions. In Proceedings of the 15th CRYPTO Conference, volume 963 of Lecture Notes in Computer Science, pages 424{437. Springer, Berlin, 1995.

[30] D. Deutsch, Proc. R. Soc. London A 400, 97 (1985).

[31] D. Meyer. Quantum games and quantum algorithms. In Quantum Computation and Quantum Information Science, Contemporary Mathematics Series. American Mathematical Society, 2001. To appear.

[32] Davis, M. (2003), 'The myth of hypercomputation', in C. Teuscher (ed.), Alan Turing, Life and Legacy of a Great Thinker, New York: Springer, pp. 195–212.

[33] E. Bernstein and U. Vazirani. Quantum complexity theory. SIAM Journal on Computing, 26(5):1411{1473, 1999

[34] http://www.ibm.com/developerworks/library/quant/index.html.

[35] J. Balc_azar, J. D__az, and J. Gabarr_o. Structural Complexity I, volume 11 of EATCS Monographs on Theoretical Computer Science. Springer, 1988.

[36] L. Adleman, J. DeMarrais, and M. Huang. Quantum computability. SIAM Journal on Computing, 26(5):1524{1540, 1997.

[37] L. Fortnow. The role of relativization in complexity theory. Bulletin of the European Association for Theoretical Computer Science, 52:229{244, February 1994.

[38] L. Li. On the counting functions. PhD thesis, University of Chicago, 1993. Department of Computer Science TR 93-12.

[39] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, United Kingdom, 2000.

[40] P. Domokos, J.M. Raymond, M. Brune and S. Haroche, Phys. Rev. A 52, 3554 (1995).

[41] P.W. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), p. 124 (1994).

[42] R. Aleliunas, R. Karp, R. Lipton, L. Lov_asz, and C. Racko_. Random walks, universal traversal sequences, and the complexity of maze problems. In Proceedings of the 20th IEEE Symposium on Foundations of Computer Science, pages 218{223. IEEE, New York, 1979.

[43] R. Landauer, Trans. R. Soc. London, Ser. A 353, 367 (1995).

[44] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof veri_cation and the hardness of approximation problems. Journal of the ACM, 45(3):501{555, May 1998.

[45] S. Fenner, F. Green, S. Homer, and R. Pruim. Determining acceptance possibility for a quantum computation is hard for PH. Technical Report 98-008, Computer Science Department, Boston University, 1998.

[46] S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder's toolkit. In Proceedings of the 8th IEEE Structure in Complexity Theory Conference, pages 120{131. IEEE, New York, 1993.

[47] Shor, P. (1994) 'Algorithms for quantum computation: Discrete logarithms and factoring', *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124–134.