RESEARCH ARTICLE OPEN ACCESS

Understanding the Fundamentals of Quantum Computing

Yew Kee Wong
JiangXi Normal University, Jiangxi - China

ABSTRACT
Quantum theory is one of the most successful theories that have influenced the course of scientific progress during the twentieth century. It has presented a new line of scientific thought, predicted entirely inconceivable situations and influenced several domains of modern technologies. There are many different ways for expressing laws of science in general and laws of physics in particular. Similar to physical laws of nature, information can also be expressed in different ways. The fact that information can be expressed in different ways without losing its essential nature, leads for the possibility of the automatic manipulation of information. All ways of expressing information use physical system, spoken words are conveyed by air pressure fluctuations: "No information without physical representation". The fact that information is insensitive to exactly how it is expressed and can be freely translated from one form to another, makes it an obvious candidate for fundamentally important role in physics, like interaction, energy, momentum and other such abstractors. This is a project report on the general attributes of Quantum Computing and Information Processing from a layman's point of view.

***Keywords* — c**omputation, EPR, quantum mechanics, superposition, unitary transformation, decoherence.

I. INTRODUCTION

With the development of science and technology, leading to the advancement of civilization, new ways were discovered exploiting various physical resources such as materials, forces and energies. The history of computer development represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage and eventual creation of the first computer by German engineer Konard Zeise in 1941. The whole process involved a sequence of changes from one type of physical realization to another from gears to relays to valves to transistors to integrated circuits to chip and so on. Surprisingly however, the high speed modern computer is fundamentally no different from its gargantuan 30 ton ancestors which were equipped with some 18000 vacuum tubes and 500 miles of wiring [1]. Although computers have become more compact and considerably faster in performing their task, the task remains the same: to manipulate and interpret an encoding of binary bits into a useful computational result.

The number of atoms needed to represent a bit of memory has been decreasing exponentially since 1950. An observation by Gordon Moore in 1965 laid the foundations for what came to be known as "Moore's Law" – that computer processing power doubles every eighteen months [2]. If Moore's Law is extrapolated naively to the future, it is learnt that sooner or later, each bit of information should be encoded by a physical system of subatomic size. As a matter of fact this point is substantiated by the survey made by Keyes in 1988 as shown in fig. 1. This plot shows the number of electrons required to store a single bit of information. An extrapolation of the plot suggests that we might be within the reach of atomic scale computations with in a decade or so at the atomic scale however.

With the size of components in classical computers shrinking to where the behaviour of the components, is practically dominated by quantum theory than classical theory, researchers have begun investigating the potential of these quantum behaviours for computation. Surprisingly it seems that a computer whose components are all to function in a quantum way are more powerful than any classical computer can be [3]. It is the physical limitations of the classical computer and the possibilities for the quantum computer to perform certain useful tasks more rapidly than any classical computer, which drive the study of quantum computing.

A computer whose memory is exponentially larger than its apparent physical size, a computer that can manipulate an exponential set of inputs simultaneously – a whole new concept in parallelism; a computer that computes in the twilight (space like) zone of Hilbert Space (or possibly a higher space – Grassman Space & so on), is a quantum computer [4]. Relatively few and simple concepts from quantum mechanics are needed to make quantum computers a possibility. The subtlety has been in learning to manipulate these concepts. If such a computer is inevitability or will it be too difficult to build on, is a million dollars question.

II. HISTORY OF QUANTUM COMPUTING

The idea of computational device based on quantum mechanics was first explored in the 1970's and early 1980's by physicists and computer scientists such as Charles H. Bennet of the IBM Thomas J. Watson Research Centre, Paul A. Beniof of Arogonne National Laboratory in Illinois, David Deustch of the University of Oxford and Richard [6, 7]

P. Feynman of Caltech. The idea emerged when scientists were pondering on the fundamental limits of computation. In 1982 Feynman was among the fewer to attempt to provide conceptually a new kind of computers which could be devised based on the principles of quantum physics [8]. He constructed an abstract model to show how a quantum system could be used to do computations and also explain how such a machine would be able to act as a simulator for physical problems pertaining to quantum physics. In other words, a physicist would have the ability to carry out experiments in quantum physics inside a quantum mechanical computer. Feynman further analysed that quantum computers can solve quantum mechanical many body problems that are impractical to solve on a classical computer [9]. This is due to the fact that solutions on a classical computer would require exponentially growing time where as the whole calculations on quantum computer can be done in polynomial time [10].

Later, in 1985, Deutsch realized that Feynman assertion could eventually lead to a general-purpose quantum computer [11]. He showed that any physical process, in principle could be modelled perfectly by a quantum computer. Thus, a quantum computer would have capabilities far beyond those of any traditional classical computer. Consequently efforts were made to find interesting applications for such a machine. This did not lead to much success except continuing few mathematical problems. Peter Shor in 1994 set out a method for using quantum computers to crack an important problem in number theory which was namely factorisation [12]. He showed how an ensemble of mathematical operations, designed specifically for a quantum computer could be organized to make such a machine to factor huge numbers extremely rapidly, much faster than is possible on conventional computers. With this breakthrough, quantum computing transformed from a mere academic curiosity directly to an interest world over.

Perhaps the most astonishing fact about quantum computing is that it took exceedingly large time to take off [13]. Physicists have known since 1920's that the world of subatomic particles is a realm apart, but it took computer scientists another half century to begin wondering whether quantum effects might be harnessed for computation. The answer was far from obvious.

III. THE ART OF QUANTUM COMPUTING

A. *Public Key Cryptography and Classical Factoring of Big Integers*

In 1970 a clever mathematical discovery in the shape of "public key" systems provided a solution to key distribution problem [14]. In these systems users do not need to agree on a secret key before they send the message. The principle of a safe with two keys, one public key to lock it, and another private one to open it, is employed. Everyone has a key to lock the safe but one person has a key that will open it again, so anyone can put a message in the safe but only one person can take it out. In practice the two keys are two large integer numbers [15]. One can easily derive a public key from a private key but not vice versa. The system exploits the fact that certain mathematical operations are easier to perform in one direction that the other e.g. multiplication of numbers can be performed much faster than factorising a large number. What really counts for a "fast" algorithm is not the actual time taken to multiply a particular pairs of numbers but the fact that the time does not increase too sharply when we apply the same method to ever-large numbers [16]. We know that multiplication requires little extra time when we switch from two three digit numbers to two thirty digit numbers using the simpler trial division method about 10□13 times more time or memory consuming than factoring a three digit number [17]. In case of factorisation the use of computational resources is enormous when we keep on increasing the number of digits. As a matter of fact public key cryptosystems could avoid key distribution problem. However their security depends upon unproven mathematical assumptions such as the difficulty of factoring large integers. Nevertheless one such protocol is RSA, which maps electronic banking possible by assuming banks and their customers that a bogus transfer of funds or a successful forgery would take the world's fastest computer millions of years to carry out. Another is the under spread Data Encryption Standard (DES) which remains secure far most ordinary business transactions [18, 19].

The procedure of factorising a large integer can be quantified as follows. Consider a number N with L decimal digits (N ~ 10 to power L). The number is factored using trial division method [20, 21]. On conventional computers one of well known]] factoring algorithm runs for number of operations of the order of

$$s \sim O(\exp((64/9)^{1/3} (\mathit{ln} N)^{1/3} (\mathit{ln}\ \mathit{ln} N)^{2/3}))$$

or explicitly, $s \sim A \exp(1.9\, L^{1/3} (\mathit{ln} L)^{2/3})$

This algorithm therefore, scales exponentially with the input size log N (log N determines the length of the input [22]. The base of the logarithm is determined by our numbering system. Thus base 2 gives the length in binary, a base 2 gives the length in binary, a base of 10 in decimal and so on) e.g. in 1994 a 129 digit number (known as RSA 129) was successfully factored using this algorithm on approximately 1600 workstations scattered around the world, the entire factorisation took eight months [23]. Using this to estimate the per factor of the above exponential scaling, it is found that it would take roughly 800,000 years to factor a 250 digit number with the same computer power, similarly a 1000 digit number would require 10 to the power 25 years (much longer than the age of universe) [24]. The difficulty of factoring large numbers is crucial for public key cryptography such as used in banks around 250 digits. Using the trial division method for factorisation $10^{L/2}$ (=□N) divisions are needed to solve the problem on exponential increase as function of L. Suppose a computer performs 10^{10} decisions per second [25]. Thus the computer can factor any number N, in about e.g. a 100 digit number will be factored in 10^{40} seconds, much longer than 3.8 X 10^{17} second (12 billion years), the currently estimated age of the universe! [26]

B. Quantum Factoring

From the analysis of classical factoring of big integers it seems that factoring big numbers will remain beyond [27] the capabilities of any realistic computing devices and unless mathematicians or computer scientists come up with an efficient factoring algorithm, the public key crypto systems will remain secure. However it turns out that this is not the case [28]. The Classical Theory of Computation is not complete simply because it does not describe all physically possible computations. In particular, it does not describe computations, which can be performed by quantum devices. Indeed, recent work in quantum computation shows that a quantum computer can factor much faster than any classical computer. According to an algorithm developed by Peter Shor factoring an integer using quantum computer runs in O((*ln*N) $^{2+□}$) steps, where □ is small [29]. This is roughly quadratic in the input size, so factoring a 1000 digit number with such an algorithm would require only few million steps. The implication is that public key cryptosystems based on factoring may be breakable.

C. Searching of an item with desired property

Searching of an item with desired property from a collection of N items is another problem that admits tremendous speed up using quantum logic based algorithm. Suppose we pick up an item at random from a collection of N items likelihood of correct selection is the same as that of right one [30], the probability of right selection is half. Hence on an average we require N/2 operations for getting the right item. However Grover invented quantum logic based algorithm, which accomplishes the same task in an average of √ N number of operations.

D. Simulation of Quantum System by Classical Computer

Richard P. Feynman, in 1982 proposed that a quantum physical system of N particles with its quantum probabilities can not be simulated by the usual computer without an exponential slowdown in the efficiency of simulation. However, a system of N particles in classical physics can be simulated with a polynomial slowdown. The main reason for this is that the description size of a particle system is linear in N in classical physics but exponential in N according to quantum computer (computer based on the laws of quantum mechanics) can avoid the slowdown encountered in the simulation process of quantum systems. Feynman also addressed the problem of simulating a quantum physical system with a probabilistic computer but due to interference phenomena, it appears to be a difficult problem.

IV. QUANTUM COMPUTING - PARALLELISM

Performing mathematical calculations, searching the internet, modelling the national economy, forecasting the weather and so on puts a constraint on the capacity of even the fastest and most powerful computers. The difficulty is not so much that microprocessors are too slow; it is that computers are inherently inefficient. Modern (classical) computers operate according to programs that divide a task into elementary operations, which are then carried out serially, one operation at a time. Efforts have been made to coax two or more computers (or at least two or more microprocessors) to work on different aspects of a problem at the same time, but the progress in such parallel computing has been slow and fitful. The reason to a large extent is that the logic built into microprocessors is inherently serial (normal computers sometimes appear to be doing many tasks at once, such as running both a word processor and spreadsheet programme, but in reality, the central processor is simply cycling rapidly from one task to the next).

In a true sense, parallel computer would have simultaneity built into its very nature. It would be able to carry out many operations at once, to search instantly through a long list of possibilities and point out the one that solves the problem. Such computers do exist. They are called quantum computers. In reality, the more exciting feature of quantum computing is quantum parallelism. A quantum system in general is not in one "classical state" but in a "quantum state" consisting (broadly speaking) in a superposition of many classical or classical like states. This is called principle of linear superposition used to construct quantum states. If the superposition can be protected from unwanted entanglement with its environment (known as decoherence) a quantum computer can output results depending on details of all its classical like states. This is quantum parallelism- parallelism on a serial machine.

V. QUANTUM SUPERPOSITIONS AND QUANTUM INTERFERENCE: CONCEPTUAL VISUALISATION OF QUANTUM COMPUTER

In a quantum computer the fundamental unit of information (is called a quantum bit or "qubit", analogous to classical bit used in ordinary computer), is not binary but rather more quaternary in nature. This qubit property arises as direct consequence of its adherence to the laws of quantum motions. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical state bit but also in states corresponding to a blend of superposition of those classical states. In other words a qubit can exist as a zero, a one, or simultaneously as both 0 and 1, with numerical coefficient representing the probability for each state. This concept may appear to be counterintuitive because every day phenomenon is governed by classical physics, not quantum mechanics, which taps out at the atomic level. Physically qubit can be visualized by the spin s=1/2 of one electron system, the two state +1/2 and –1/2 being two eigenstates of S_z (z component direction of an external magnetic field of spin ½.).

Alternatively a beam of single photon can also be used, the total states being the state of polarization (horizontal or vertical) with respect to some chosen axis. Thus qubit can take 2 values, 0 or 1, which are associated with two eigenstates of a spin of a single electron (say):

|1> = |↑>
|0> = |↓>

|0> + |1> = |↑> + |↓>

And further qubit can be a superposition of these two states with complex coefficient and this property distinguishes them form classical bits used in conventional computers. In mathematical terms, we say that since the general state of a qubit can be superposition of two pure states with arbitrary complex coefficients, then the state is described as a vector in the two dimensional complex space c^2 and the two pure states form the basis of the representation.

This can be demonstrated by placing an absorbing screen in the way of either of the routes, then it becomes equally probable that detector A or B is reached. Block of one of the paths actually allows detector B to be reached; with both routes open, the photon somehow knows that it is not permitted to reach detector B, so it must have actually felt out both routes. It is therefore perfectly legitimate to say that between the two half silvered mirrors the photon took both transmitted and reflected paths or using more technical language, we can say that photon is in a coherent superposition of being in the transmitted beam and in the reflected beam. This quantum interference is resulting due to linear superposition principle. This is one of those unique characteristics that make current research in quantum computing not merely a continuation of today's idea of computer but rather an entirely new branch of thought and underlying concept and it is because quantum computers harness those special characteristics that gives them the potential to be incredibly powerful computational device.

VI. CONCLUSION

The foundations of the subject of quantum computation have become well established, but everything else required for its future growth is under exploration. That covers quantum algorithms, logic gate operations, error correction, understanding dynamics and control of decoherence, atomic scale technology and worthwhile applications. Reversibility of quantum computation may help in solving NP problems, which are easy in one direction but hard in the opposite sense. Global minimization problems may benefit from interference effects (as seen in Fermat's principle in wave mechanics). Simulated annealing methods may improve due to quantum tunneling through barriers. Powerful properties of complex numbers (analytic functions, conformal mappings) may provide new algorithms. Theoretical tools for handling many-body quantum entanglement are not well developed. Its improved characterization may produce better implementation of quantum logic gates and possibilities to correct correlated errors.

Though decoherence can be described as an effective process, its dynamics is not understood but an attempt has been made in the present project work in the form of Symmetry breaking argument or need for an entropy like parameter or function to account for irreversibility in the system. To be able to control decoherence, one should be able to figure out the eigenstates favored by the environment in a given setup. The dynamics of measurement process in not understood fully, though the attempt is also made in this regard in this project. Measurement is just described as a non-unitary projection operator in an otherwise unitary quantum theory. Ultimately both the system and the observer are made up of quantum building blocks, and a unified quantum description of both measurement and decoherence must be developed. Apart from theoretical gain, it would help in improving the detectors that operate close to the quantum limit of observation. For the physicist, it is of great interest to study the transition from classical to quantum regime. Enlargement of the system from microscopic to mesoscopic levels, and reduction of the environment from macroscopic to mesoscopic levels, can take us there. If there is something beyond quantum theory lurking, there it would be noticed in the struggle for making quantum devices. We may discover new limitations of quantum theory in trying to conquer decoherence. Theoretical developments alone will be no good without a matching technology. Nowadays, the race for miniaturization of electronic circuits in not too far away from the quantum reality of nature. To devise new types of instruments, we must change our view-points from scientific to technological-quantum effects which are not for only observation; we should learn how to control them for practical use. The future is not foreseen yet, but it is definitely promising.

REFERENCES

[1] K. Brading, and E.Castellani, "Symmetries in Physics: Philosophical Reflections, Cambridge University Press, 2003.

[2] Sanjeev Kumar, "Reformulation of Classical Electrodynamics", Jiwaji University, Gwalior, India.

[3] A. Barredo Arrieta, N. Díaz-Rodríguez, J. Del Ser et al., "Explainable Artificial Intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020.

[4] Y. Song, Y. Fu, F. R. Yu et al., "Blockchain-enabled internet of vehicles with cooperative positioning: a deep neural network approach," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3485– 3498, 2020.

[5] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. Obaidat, and B. Sadoun, "Habits: blockchain-based telesurgery framework for healthcare 4.0," in *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, IEEE, Beijing China, August 2019.

[6] J. Wang, C. Jiang, H. Zhang, Y. Ren, and K-C. Cheng, "Thirty years of machine learning: the road to Pareto-optimal wireless networks," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1472–1514, 2020.

[7] W. Sun, N. Xu, L. Wang, H. Zhang, and Y. Zhang, "Dynamic digital twin and federated learning with incentives for air-ground networks," *IEEE Transactions on Network Science and Engineering*, p. 1, 2020.

[8] Wang, C. Jiang, K. Zhang, T. Q. S. Quek, Y. Ren, and L. Hanzo, "Vehicular sensing networks in a smart city: principles, technologies and applications," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 122–132, 2017.

[9] Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the internet of things (IoT) in smart logistics: a comprehensive survey," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.

[10] H. Cao, L. Yang, and H. Zhu, "Novel node-ranking approach and multiple topology attributes-based embedding algorithm for single- domain virtual network embedding," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 108–120, 2017.

[11] T. Yang, Z. Jiang, R. Sun, N. Cheng, and H. Feng, "Maritime search and rescue based on group mobile computing for UAVs and USVs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7700–7708, 2020.

[12] T. Yang, H. Feng, S. Gao et al., "Two-stage offloading optimization for energy-latency tradeoff with mobile edge computing in maritime Internet of Things," *IEEE Internet of Things Journal*, vol. 7, pp. 5954– 5963, 2019.

[13] P. Guo, W. Hou, L. Guo, Z. Cao, and Z. Ning, "Potential threats and possible countermeasures for photonic network-on-chip," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 48–53, 2020.

[14] X. Hou, Z. Ren, J. Wang et al., "Reliable computation offloading for edge computing-enabled software-defined IoV," *IEEE Internet of Things Journal*, vol. 7, pp. 7097–7111, 2020.

[15] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: sensing-aided transportation information collection and diffusion," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3813–3825, 2018.

[16] J. Guo, Y. Zhou, P. Zhang, B. Song, and C. Chen, "Trust-aware recommendation based on heterogeneous multi-relational graphs fusion," *Information Fusion*, vol. 74, pp. 87–95, 2021.

[17] M. B. Mollah, J. Zhao, D. Niyato et al., "Blockchain for the internet of vehicles towards intelligent transportation systems: a survey," *IEEE Internet of Things Journal*, vol. 8, pp. 4157–4185, 2020.

[18] J. Feng, F. R. Yu, Q. Pei, J. Du, and L. Zhu, "Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 4321–4334, 2020.

[19] Z. Zheng, S. Xie, H. N. Dai, X. Cheng, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[20] S. Hu, Y. C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond," *IEEE Wireless Communications*, vol. 99, pp. 1–7, 2021.

[21] X. Cai, Y. Ren, and X. Zhang, "Privacy-protected deletable blockchain," *IEEE Access*, vol. 8, pp. 6060–6070, 2019.

[22] M. Á. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "PUF-derived IoT identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, Article ID 100057, 2020.

[23] W. Sun, S. Lei, L. Wang, Z. Liu, and Y. Zhang, "Adaptive federated learning and digital twin for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5605–5614, 2020.

[24] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and J. Piran, "Blockchain- based incentive energy-knowledge trading in IoT: joint power transfer and AI design," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.

[25] M. I. Mehar, C. L. Shier, A. Giambattista et al., "Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack," *Journal of Cases on Information Technology*, vol. 21, no. 1, pp. 19–32, 2019.

[26] G. Raja, Y. Manaswini, G. D. Vivekanandan et al., "AI-powered blockchain-a decentralized secure multiparty computation protocol for IoV," in *Proceedings of the conference IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 865–870, IEEE, Toronto, ON, Canada, August 2020.

[27] M. Gawas, H. Patil, and S. S. Govekar, “An integrative approach for secure data sharing in vehicular edge computing using Blockchain,” *Peer-to-Peer Networking and Applications*, pp. 1–9, 2021.

[28] M. B. Mollah, J. Zhao, D. Niyato et al., “Blockchain for future smart grid: a comprehensive survey,” *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.

[29] P. K. Sharma, N. Kumar, and J. H. Park, “Blockchain-based distributed framework for automotive industry in a smart city,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4197–4205, 2018.

[30] T. Baltrušaitis, C. Ahuja, and L. P. Morency, “Multimodal machine learning: a survey and taxonomy,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 2, pp. 423–443, 2018.