Principle and State-of-Art Applications of Quantum Computing

Guixi Wu *

Chengdu Experimental Foreign Language School West Campus, Chengdu, China

* Corresponding Author Email: sherlock1412@ldy.edu.rs

Abstract. Contemporarily, the classical computing has met the upper limitations of Moore's law due to the restrictions of the resolution for light sourcing and material. On this basis, the quantum computing has been rapidly developed due to the advantages of parallel computation, which is able to be faster more than 3 orders of magnitude than conventional computer in some issues. With this in mind, this study discusses the basic principles of quantum computing as well as the corresponding state-of-art applications. To be specific, the developing history of the quantum computing is briefly introduced. Subsequently, the entanglement principle will be demonstrated accordingly. Afterwards, three types of the state-of-art quantum computing facilities will be demonstrated. Then, some of the applications and common algorithms will be discussed simultaneously. According to the analysis, the limitations and defects of current investigation of quantum computing will be illustrated. In conclusion, these outcomes provided guideline for further exploration of quantum computing.

Keywords: Quantum computing; entanglement; algorithms.

1. Introduction

Ever since the advent of humans, computing has been an important proposition in human life. In ancient times, various countries and peoples developed various ways to assist in calculations, such as the Chinese abacus and the European mechanical calculator [1, 2]. In 1946, ENIAC (The Electronic Numerical Integrator And Computer) was released in Philadelphia, which marked the birth of modern computers [3]. Since then, humans have begun to move rapidly on the road to large-scale rapid computing. From tubes to transistors, from integrated circuits to LSIs. The computer iterates at a very fast rate. It's getting more powerful and smaller. In 1965, Due to the rapid pace of development in the field of computing, Gordon Moore, one of Intel's founders, raised Moore's Law. It illustrates that if the price does not change, the amount of components that can be accommodated on the comprehensive circuit will double every 1.5-2 years, ao as to performance. In other words, every dollar of computer showcase will more than double every 1.5-2 years. This law indicates an acceleration in the speed at which information technology.

However, with the subsequent development of technology and chip integration, the application of traditional semiconductors is now close to the performance limit of materials. In order to continue to develop, one urgently needs to seek new breakthroughs at the theoretical level. In 1982, in his esteemed lecture, Richard Feynman envisaged a quantum machine based on the principles of quantum mechanism simulating quantum physics, which was regarded as one of the first concepts of quantum computing (QC) in many aspects. He hypothesized that nature is not classical, so in order to simulate natural phenomena, one needs a computing device based on the principles of quantum mechanics. His ideas pointed the way forward for the computer field in a bottleneck period.

In fact, to provide the tremendous computational power necessary for the simulation of sophisticated quantum systems, quantum computers offer the possibility for computation to take advantage of quantum mechanical characteristics, such as entanglement and superposition. Since the suggested quantum mechanical characteristics remain a very fundamental natural scale, initial progress in improving quantum computer hardware has been relatively tardy.

2. Principle of Quantum Computing

Quantum computing relies on the nature of quantum information processing. Information presentation by a quantum system depends on structures like quantum bits and quantum gates as well

as operations and principle such as observation, non-cloning theorem, and quantum teleprotation. Quantum bit, or abbreviated as qubit, is a two level quantum system. Traditionally, it is described as a two-dimensional Hilbert Space equipped with basis, $\{|0\rangle, |1\rangle\}$. The general state of a single qubit is a unit-length vector of the form

$$c_0|0\rangle+c_1|1\rangle, \tag{1}$$

where $c_0, c_1 \in \mathbb{C}$ and $|c_0|^2 + |c_1|^2 = 1$. c_0, c_1 are called the amplitudes of states $|0\rangle$, $|1\rangle$,respectively. Observation of a qubit gives result of either 0 or 1 with probabilities $|c_0|^2$and$|c_1|^2$.

Mathematically, system with multiple qubits is described by tensor product of multiple systems. However, there exists some multi-qubit states that cannot be described by tensor product of qubits, such states are called entangled states. EPR pair [4], which has the form

$$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle, \tag{2}$$

is a typical entangled state that cannot be written as tensor product of two qubits.

Any effect acting on a quantum system, like time evolution, can be described by unitary operators. In quantum logic circuit, an operator is usually achieved by one or a group of quantum gates. A universal gate set is required to perform all unitary operation. However, for system with the more than one qubit, there is no operation to copy the state of the system to other qubits, which is also known as no-cloning theorem. Besides a universal gate set, an practical quantum system need to satisfies certain conditions, which is known as DiVincenzo criteria [5]. There are five conditions for a quantum system to be operable:

- scalable system with well-characteristic qubits
- capability to initialize qubit to simple state
- much longer coherence time than gate operations
- universal set of quantum gates
- ability to perform measurement

Transition of quantum information between quantum system is also vital to the development of quantum computing. Transferring unknown quantum states through a long distance utilizes the entanglement of qubits, which is called quantum teleportation, was first proposed in 1993 [6]. Two people Alice and Bob sharing one of each qubits in an entangled state at a long distance. Then, Alice can teleport an unknown states with the entangled state to Bob. Bob measuring his qubit repeatedly and mapping the result with a protocal. With enough measurements, Bob will get enough information to reconstruct the state that Alice teleported.

3. State-of-art Facilities

Now there are three major state-of-art facilities of quantum computer in industry. IBM Quantum is a groundbreaking IBM programme to explore and advance the field of quantum computing. It encompasses a range of activities, including research, development, and the provision of quantum computing resources for researchers, developers, and enthusiasts around the world. IBM Quantum Computing includes the development of quantum computers, which are advanced computational systems that conduct certain modes of calculations much faster than traditioinal computers by utilising the laws of quantum mechanism. IBM has made great strides in building quantum processors, with the number of quantum bits continues to increase and performance has improved. Quantum bits are the basic building blocks of a quantum computer. Unlike classical bits, which can only be 0 or 1, quantum bits can exist in a superposition of two states simultaneously. Quantum gates, similar to classical logic gates, are used to manipulate the states of quantum bits.IBM Quantum emphasises open-source collaboration.The software tools, development kits, and educational resources provided by IBM Quantum are often open-source, allowing the quantum community to contribute, learn, and build on existing work.

In addition to hardware development, IBM Quantum focuses on quantum software and algorithms. Quantum computing continues to be a rapidly evolving field, and researchers are exploring new algorithms to solve complex problems more efficiently using the unique properties of quantum systems.The IBM Quantum Network is a community of researchers, professionals and organisations working together to accelerate the development of quantum computing. It connects researchers with IBM's quantum expertise, tools and resources.

Google Quantum Artificial Intelligence (often referred to simply as "Google Quantum") is an initiative launched by Google to advance the field of quantum computing and explore potential applications of quantum technology. It involves research, hardware development, and collaboration with the broader quantum community. Google Quantum AI is dedicated to developing quantum processors and hardware systems capable of performing quantum computations. One of its most notable achievements was the creation of the Bristlecone quantum processor, which was one of the first processors to have enough quantum bits to demonstrate quantum supremacy - the ability of a quantum computer to complete certain tasks faster than traditional one. In 2019, Google Quantum AI published a landmark paper on quantum supremacy, demonstrating that their Bristlecone processor can perform a specific type of quantum computation that is practically impossible for a classical computer to emulate in a reasonable timeframe. This marks a major breakthrough in quantum computing. Google Quantum AI researchers explore and develop new algorithms that utilize the special characteristics of quantum systems to address complicated problems more efficiently than traditional computers. These algorithms can be applied in fields such as cryptography, optimization, and machine learning.

Jiuzhang is the first light-based quantum computer. Jiuzhang is often described as a "boson sampling" quantum computer. Instead of using conventional quantum bits (such as those found in superconducting or ion-trap quantum computers), Jiuzhang uses photons as quantum bits. These photons are manipulated in complex optical paths to perform quantum computations. It performs boson sampling, a quantum computing task that involves sending multiple photons through a specialised optical path called an interferometer. These photons interact and interfere with each other in ways that encode solutions to mathematical problems. The final measurement of the photon positions provides information about the solution. A sketch of the Jiuzhang is shown in Fig. 1.

Fig. 1 A sketch of Jiuzhang.

4. Applications

The idea of quantum computing was first raised by Richard Feynman, in order to settle the difficulty of imitating physically diverting quantum systems with traditional computers. The general concept of a quantum simulation computer is to create a known quantum state, explore it under a Hamiltonian mimicking a physical system of interest, and measure visualized quantities of the ultimate wave-function. Suggestions for interesting problems to imitate quantum computers involve

quantum phase transitions, high temperature superconductivity, chemical reactions, and even more exotic phenomena such as Hawking radiation [7].

There are about three applications of quantum computing. Quantum computing has the potential to have a major impact on cryptography and security. In 1994, Peter Shor discovered the dominant factors of Shor's algorithm for the first time [7]. Depending on the assumption that prime large factoring amounts is an intractable problem, primary factorization is an pivotal problem for plentiful current encryption protocols. However, Shor's calculating system scales polynomially, unlike the prestigious traditional algorithms scaling nearly exponentially with the quantity of digits. As a result, Shor's calculating system illustrates that quantum computing could offer exponential speedups in problems with real-world consequences, and has historically been a dominant booster for funding quantum computer research [8]. Fig. 2 is a typical results. This has implications for breaking widely used public key cryptosystems such as RSA. Quantum Key Distribution (QKD), such as the BB84 protocol, provides a more secure method of exchanging encryption keys using quantum mechanical principles to ensure that eavesdropping is detected. Anti-quantum encryption methods are also being explored to defend against potential threats from quantum computers.

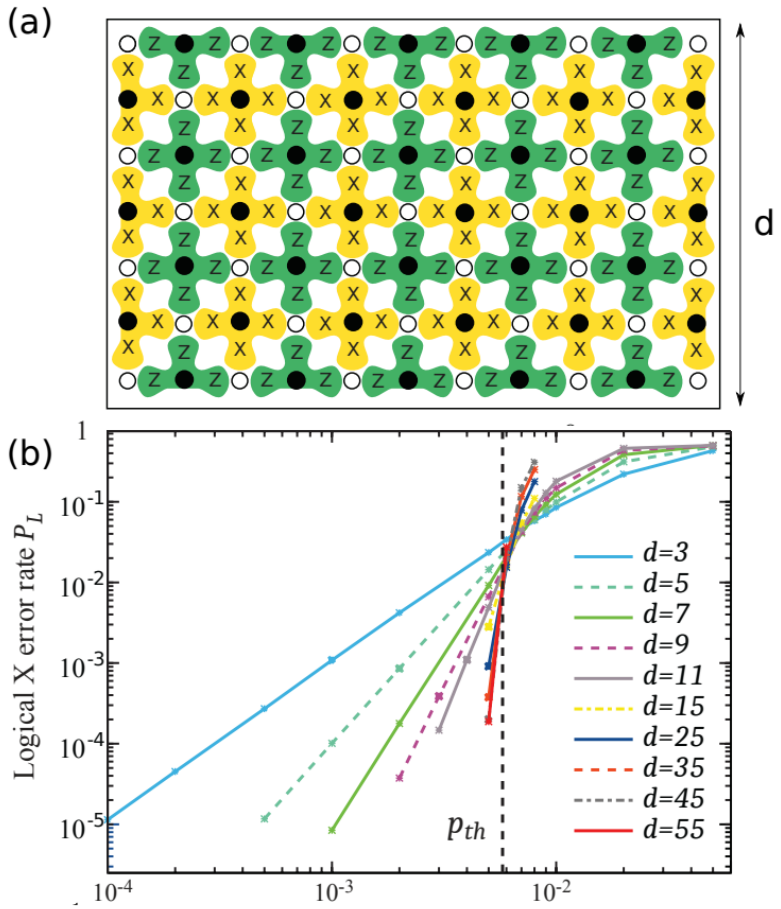

Fig. 2 Typical results of quantum computing.

Quantum computers excel at solving complex optimization problems. Grover's calculating method works by utilizing amplitude extension [9]. Grover's calculating system selectively and iteratively enhances the scope of |x⟩ from an equal superposition of N states constructed utilizing n=log2N qubits. The ultimate scaled state will be |x⟩ with high potential by giving enough iterations. Being a quadratic speed up over a brute force traditional search, the quantity of iterations requested for Grover's calculating system measures as N. For example, they can be used to optimize supply chains, financial portfolios, energy distribution, and more. Quantum annealing is a specialized quantum optimization technique that has been proposed for solving optimization problems and minimizing energy functions. Quantum computing can also imitate quantum methods more efficiently than traditional computing

methods, which has applications in materials science, drug discovery, and fundamentally understanding chemical reactions.

Artificial Intelligence and Machine learning: Quantum computing is possible to reinforce machine learning and artificial intelligence calculating systems. Quantum computers can efficiently conduct linear algebra operations, which are the basis of many machine learning algorithms. Quantum algorithms of machine learning such as quantum neural networks and quantum based vector machines have been proposed to increase the speed and capability of AI tasks. Quantum computers can also process large data sets more efficiently and deal with more complex models, leading to potential breakthroughs in the field of AI research.

5. Limitations and Prospects

For now, though quantum computers has been fabricated and run by Techs like Google and IBM, it is still restricted for more general use. Current quantum computers are restricted to merely few qubits, which is not useful to solve computational problems. As quantum computer suffers from the difficulty to scale up, on the one hand, current techniques implement superconducting and structures like Josephson junction to fabricate qubits, which requires ultracold environment temperature and hence increase the cost. Though superconducting qubits can utilize well-established microfabrication process to scale up, the accuracy of such a quantum computer is still too low. On the other hand, method like ion traps achieve higher accuracy and longer coherence, but suffer from the low maturity of fabrication. Nevertheless, effort addressing these issues has been proposed. Work focusing on improving accuracy has been widely studied in quantum error correction. Classical three-bit encoding is also utilized for error detection. Meanwhile, extra qubits are used to indicate the type of errors in the circuit, such qubits are called syndrome qubits. Decades ago, Shor code provides method encodes 1 logical qubit into 9 physical qubits that can correct arbitrary error in single qubit [10], and practice on fault tolerant control of error-corrected qubit has been researched [11].

A promising way to deal with the difficulty of integrating ion trap to current chip manufacture process is surface electrode ion trap. The ion trap scheme satisfies the five requirements for a quantum computer outlined by DiVincenzo and validated in several laboratories: (1) a scalable system consisting of well-defined quantum bits, (2) a way to reliably initialise the quantum system, (3) long coherence times, (4) the existence of universal gates, and (5) an efficient measurement scheme [12]. The surface electrode ion trap junction is a key element of large-scale ion trap array [12]. It is a device for trapping, manipulating and storing ions and is commonly used in quantum computing and quantum information processing research. Points that are more advantageous than traditional three-dimensional ion traps are (1) surface-electrode ion traps are usually made of a flat chip with an electrode structure that generates an electric field to trap and manipulate single or multiple ions, making them easier to integrate; (2) Surface-electrode ion traps can also form long-lived ion bits, which makes them more stable by allowing more calculations to be performed and less likely to lose quantum information.

6. Conclusion

To conclude, the development of computing has seen tremendous revolution from ancient to modern times, and quantum computing emerged due to the limitations of traditional computing methods. Before introducing five conditions of an operable quantum system, the principles of single qubit and multi-qubits were illustrated. The transition of quantum information between quantum systems is also vital to the development of quantum computing. There are three major state-of-art facilities of quantum computers in industry, including IBM Quantum, Google Quantum, and "boson sampling" Quantum. Additionally, Cryptography and Security, Optimization and simulation as well as Machine learning and Artificial Intelligence are three main applications of quantum computing, the characteristics of which were discussed in the essay. For now, quantum computers are restricted

to general use, with disadvantages appearing in the current quantum technology. The importance of addressing this problem lies in improving the accuracy of quantum computing.

References

[1] Rojas-Sola J I, del Río-Cidoncha G, Fernández-de la Puente Sarriá A, et al. Blaise pascal's mechanical calculator: Geometric modelling and virtual reconstruction. Machines, 2021, 9(7): 136.

[2] Gomez-Jauregui V, Gutierrez-Garcia A, González-Redondo F A, et al. Torres Quevedo's mechanical calculator for second-degree equations with complex coefficients. Mechanism and Machine Theory, 2022, 172: 104830.

[3] Brainerd J G. Genesis of the ENIAC. Technology and Culture, 1976, 17(3): 482-488.

[4] Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete. Physical review, 1935, 47(10): 777.

[5] DiVincenzo D P. The Physical Implementation of Quantum Computation. Fortschritte der Physik, 2000, 48(9–11): 771–83.

[6] Shor, Peter W. "Scheme for reducing decoherence in quantum computer memory". Physical Review A, 1995, 52(4).

[7] Chen Z. Metrology of quantum control and measurement in superconducting qubits. University of California, Santa Barbara, 2018.

[8] Grover L K. Quantum Mechanics Helps in Searching for a Needle in a Haystack. Physical Review Letters, 1997, 79(2): 325–328.

[9] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994: 124–34.

[10] Egan L, Debroy D M, Noel C, et al. Fault-tolerant control of an error-corrected qubit. Nature, 2021, 598(7880): 281-286.

[11] Wineland D J, Barrett M, Britton J, et al. Quantum information processing with trapped ions. Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 2003, 361(1808): 1349-1361.

[12] Zhang C, Mehta K K, Home J P. Optimization and implementation of a surface-electrode ion trap junction. New Journal of Physics, 2022, 24(7): 073030.