The fundamental theory of quantum computing, applications in practical fields, and future challenges

Shengyu Hung

The State University of New York at Stony Brook, 300 Circle Rd, Stonybrook, NY 11790, USA

shengyuhung0329@gmail.com

Abstract. Building on the fundamental principles of quantum computing, this paper sequentially presents the development of quantum computing and its associated application domains. We also analyze and compare the differences between quantum and classical computing, highlighting the benefits of quantum computing for specific problems. To comprehend the advantages of quantum computing in particular fields, extensive research has been conducted in three areas: cryptography, chemistry, and artificial intelligence. We also discuss the wider applications of this emerging technology for future investigation, considering the current state of quantum computing development and anticipated trends.

Keywords: quantum computing, qubits, shor algorithm, grover algorithm, quantum key distribution.

1. Introduction

The concept of quantum computing was first introduced in the early 1980s by Paul Benioff of ARGONNE NATIONAL LABORATORY, who argued that quantum systems of two-energy order could emulate digital computation [1]. Subsequently, in 1981, Paul Benioff and Richard Feynman gave a talk on quantum computing at the First Conference on Computational Physics held at MIT in Boston. This conference aimed to set new requirements and goals for effective computational methods. Their talk outlined the vision of computing with quantum phenomena since Richard Feynman had observed that it seemed impossible to efficiently model the evolution of quantum systems on a classical computer, and he proposed a basic model of quantum computers [2]. And in 1982, Richard Feynman published a paper on quantum computing: "Simulating Physics with Computers" [3]. Almost a decade later, Shor's algorithm, developed by Peter Williston Shor, was introduced, and it is considered a milestone in the history of quantum computing. The algorithm allows quantum computers to decompose large integers at higher speeds and break many cryptographic systems [4]. This discovery caused great interest in quantum computing research, replacing the traditional classical computing algorithms within a few hours. Later, in 1996, Lov Kumar Grover invented the Grover database search algorithm, which demonstrated a quadratic acceleration that could solve problems that had to be solved by random brute force search and could also be applied to a broader problem base. 1998 witnessed the development of a quantum algorithm working on a 2-qubit nuclear magnetic resonance quantum computer working on the first experimental demonstration of a quantum algorithm. In the same year, an operational 3-qubit NMR quantum computer was developed, and Grover's algorithm was executed for the first time in an NMR quantum computer. Several experimental advances occurred between 1999 and 2009, and in 2009, a team at the National Institute of Standards and Technology in Colorado introduced the first general-purpose programmable quantum computer. This computer was capable of handling 2 quantum bits. Nearly a decade later, IBM launched the first commercially available integrated quantum computing system and has since added four more quantum computing systems and a newly developed 53-qubit quantum computer. Google also contributed significantly to the field in late 2019 when a paper published by a Google research team claimed to have reached quantum supremacy.

The 54-quantum-bit Sycamore processor, made of tiny quantum bits and superconducting materials, allegedly completed a calculation in just 200 seconds. And the media discovered the word quantum supremacy. They began to be publicized everywhere, which led the general public, who did not understand the word's meaning, to think it meant domination in some field. On December 4, 2020, the University of Science and Technology of China developed a quantum computer using 76 photons: the Chinese Nine-Chapter Quantum Computer. Many in the media were excited that China had succeeded in breaking the U.S. quantum supremacy or could compete with the U.S. for the title of quantum supremacy. They have misunderstood the meaning of the word. This research will be about the background and history of quantum computing, the basic principles of quantum computing, the applications of quantum computing in cryptography, chemistry, and materials science, the applications of quantum computing in optimization and machine learning, and the comparison of quantum computers with classical computers, and finally a summary will be given on the trends and future directions of quantum computers. A summary will be given at the end of the paper.

2. Related fundamental knowledge

2.1. Quantum bits and quantum entanglement

In the quantum world/computing, information is represented in quantum bits, which creates a distinction from classical bits. Classical bits represent only two states, usually denoted by 0 and 1. A classical bit is in one of the 0 or 1 states at any moment. Quantum bits, on the other hand, take advantage of the properties of quantum mechanics by adding the concept of superposition states to 0 and 1. A quantum bit can be simultaneously in 0 and 1 states, and two complex probability amplitudes determine the states.

Quantum bits also have the unique property of quantum entanglement. Entanglement means that the states of two or more quantum bits are closely related, even if they are far apart. An operation or measurement on one entangled quantum bit immediately affects another entangled quantum bit. This phenomenon does not exist in classical bits. Quantum entanglement provides tremendous parallelism and computational speed for quantum computing, leading to breakthrough applications in quantum communication and cryptography [5].

2.2. Fundamentals of quantum computing

What is commonly referred to as quantum computing is the manipulation of qubits in a superposition state through quantum logic gates. A series of arithmetic operations are performed on N qubits, and a measurement is performed. As depicted in Figure 1, N horizontal lines are drawn side by side, from left to right, representing the time order, with each line representing a different qubit. Various small squares, large squares, and vertical lines are arranged on these lines, representing single or multi-qubit operators, each called a (quantum) gate, such as the Hadamard gate (H gate). The H gate, represented by the letter H in Figure 1, has one of its main functions: generating superposition states with equal probability by processing the ground state. The whole diagram is called a quantum network/quantum circuit.

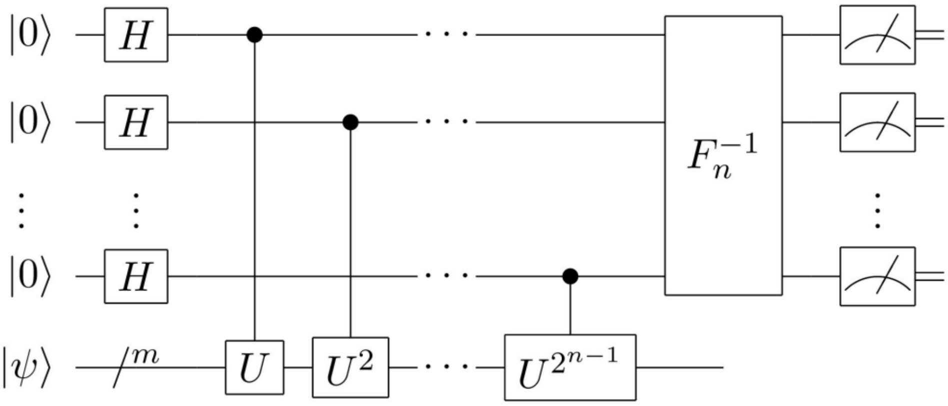

Figure 1. Principles of quantum bit computing.

2.3. Comparison of quantum computing and classical computing

Quantum computing is characterized by the parallel evolution of quantum superposition states because of the use of quantum bits, which gives quantum computing a significant advantage in computing specific problems. Assuming that 8 bits on a chip are used to store the initial parameters, 4 times 2 means there are 16 initial parameters. For a conventional computer, these four bits can only count one parameter, and if you want to count them all at once, you need 16 chips to compute them together. However, the advantage of quantum computers is their ability to superimpose 16 initial parameters simultaneously, akin to having 16 core chips. This allows for the concurrent calculation of these parameters, giving quantum computers an unparalleled edge over traditional supercomputers in terms of parallel computing capabilities. For supercomputers to increase computing speed, a meaningful way to do so is to carry out CPU stacking cores. At the same time, quantum computers do not have difficulty coordinating many chips together like supercomputers. The second advantage pertains to scalability, wherein the value of a bit is typically recorded as a binary 0 or 1. A bit can only be one of 0 or 1, but a quantum bit can be both 0 and 1 because of the quantum mechanical superposition property, as shown in Figure 2. Each quantum bit can be in two different states simultaneously, meaning that one can be used as two bits simultaneously. Using the same example of 4 bits, a conventional bit can store one number in 4 bits, while a quantum bit can store 16 numbers, equivalent to using the same space and doubling the storage capacity by 16 times [6].

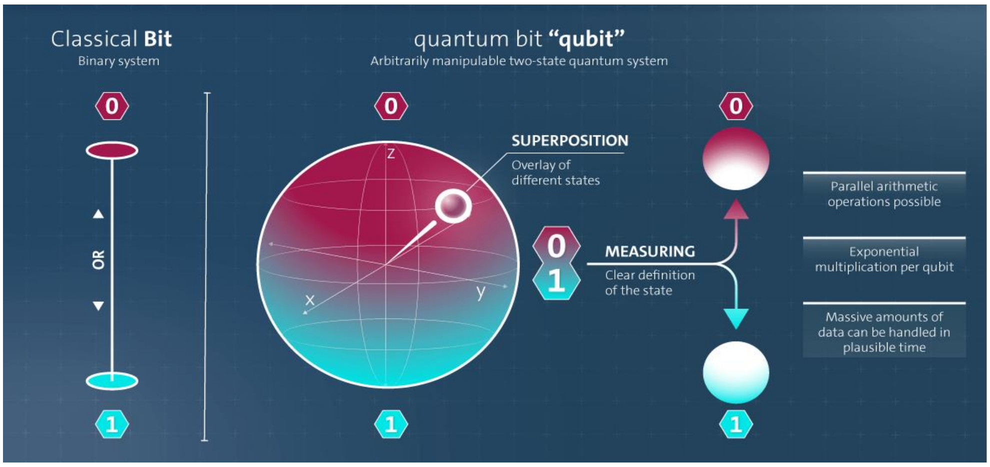
Classical Bit
Binary system
0
OR
1
quantum bit "qubit"
Arbitrarily manipulable two-state quantum system
0
z
SUPERPOSITION
Overlay of different states
x
y
1
0
1
MEASURING
Clear definition of the state
0
1
Parallel arithmetic operations possible
Exponential multiplication per qubit
Massive amounts of data can be handled in plausible time

Figure 2. Different states of quantum bits [6].

Because of the uniqueness of quantum computing, quantum computers have an inherent advantage in certain problems, such as integer factorization via Shor's algorithm and the search of unordered databases via Grover's algorithm (quantum search algorithm). Integer factorization, often called prime factorization, is an asymmetric cryptographic algorithm designed around the computational challenge of factoring large numbers into their prime components. It is an exponentially complex problem for classical computers. The most famous algorithm is Rivest-Shamir-Adleman (RSA). And Shor's algorithm can complete the large number factorization with polynomial complexity so that the RSA algorithm can be broken quickly [7]. Grover's algorithm, widely acknowledged as the second most significant quantum algorithm after Shor's algorithm, is the first to be fully implemented experimentally. It addresses the Unordered Database Search problem, which involves finding specific elements that meet certain criteria within a massive unordered database. Since the number of elements in the database is huge and unordered, verifying whether a given element satisfies the requirements is easy. Still, conversely, it is not easy to find these elements [8]. To solve the unordered database search problem (it may be assumed that there is only one target search data), the time complexity required by the classical algorithm is O(N). In contrast, the time complexity required by the Grover search algorithm is only O(N), which has a squared speedup compared to the classical algorithm, demonstrating the powerful performance of quantum computing [9].

3. Applications of quantum computing

Because quantum computing has a strong cracking advantage over Rivest-Shamir-Adleman's, and this is leading to ongoing advances in cryptography. Researchers are starting to use quantum in cryptography, and a new field like Quantum Cryptography has emerged. The basic principle of Quantum Cryptography is also different from classical cryptography in that it uses physical principles rather than mathematical operations, which allows users to ensure that their keys are not tapped. This is due to the "uncertainty principle" and "no-cloning theorem" of quantum mechanics. Currently, "Quantum Key Distribution (QKD)" is used to ensure security [10], with specific algorithmic protocols such as BB84, BBM92, EKERT91, etc. The basic principle is to pass two channels, a quantum channel, and a classical channel, and the quantum channel is used to pass the information of the quantum state. The classical channel is used to pass the necessary information to measure the quantum state. The specific steps involve sender A initially using a quantum channel to transmit the quantum state information. Next, receiver B performs a random measurement, recording the measurement and the corresponding result. Subsequently, A utilizes a classical channel to transmit their measurement and result, allowing B to compare its result with A's. If the result is the same, then it can also be considered that the bit is normal, not stolen; if comparison comes down to the same measurement but different results, it has been measured and stolen. If a hacker avoids direct measurement and instead intercepts and copies the quantum state, they would then send the original quantum state to B and retain the copied quantum state for measurement. However, due to the quantum no-cloning theorem, copying an individual quantum state would first require a measurement to be performed. The measurement necessarily changes the state of the quantum, so the hacker cannot make an accurate copy of a quantum of an unknown quantum state [11].

In 2019, Google developed the Sycamore quantum processor. In 2020, this quantum processor was successfully employed to simulate the reaction of diazole molecules with hydrogen atoms, forming alternative conformations. It accurately described the changes in hydrogen atom positions and the corresponding hydrogen chain binding energies. This achievement also signifies that precise electronic structure calculations were finally accomplished [12-13]. With the increase in the number of quantum bits and further optimization of quantum algorithms, quantum computers will make it possible to simulate more complex chemical reactions with higher efficiency and thus develop new chemical substances with shorter cycles. This is particularly important in special times, such as developing new drugs for viruses similar to COVID-19.

In artificial intelligence, the development of quantum computing offers the idea of providing a new quantum of enhanced computing power. As the number of quantum bits in a quantum computer grows exponentially, and its computational power is exponential in the number of quantum bits, this growth will be much faster than the growth of data volume, bringing a powerful hardware foundation for artificial intelligence in the era of data explosion. TensorFlow Quantum (TFQ) is an open-source library launched by Google for the rapid prototyping of quantum machine learning models TFQ is a Python framework for hybrid quantum-classical machine learning. The framework allows quantum algorithm researchers and machine learning researchers to explore combining quantum computing with machine learning for building quantum machine learning models. The core idea is interweaving quantum algorithms and machine learning programs in a TensorFlow programming model. Google refers to this approach as quantum machine learning and can implement it by leveraging some of the latest quantum computing frameworks (e.g., Google Cirq). TFQ is mainly oriented towards executing quantum circuits on classical quantum circuit simulators. In the future, TFQ will be able to execute quantum circuits on actual quantum processors supported by Cirq, including Google's own Sycamore quantum chip [14].

4. Current research directions

Quantum computing is currently in an early and rapidly evolving stage. In 2022, the hardware aspects of quantum computers focus on increasing the number, density, and connectivity of quantum bits; enhancing the quality of quantum bits, including improved coherence times and gate fidelity; designing and implementing new architectures, such as 3D configurations and novel assembly techniques; developing industrial-scale manufacturing facilities capable of assembling and integrating large quantum processors; and demonstrating interconnectivity and information exchange between different quantum computers, among other advancements. In superconducting quantum computing: IBM released the Osprey processor with 433 quantum bits, which will increase to 1000 in 2023 if it advances strictly on the technical lines [15]. In the field of Trapped Ion Quantum Computing: progress in the quality of quantum bits, increase in quantum volume, the world first in SPAM fidelity, and even more success in creativity fidelity above physical quantum bits for logical quantum bits [16]. In the field of optical quantum: the Canadian company Xanadu has successfully demonstrated the superiority of quantum computing by completing a Gaussian bosonic sampling experiment with a programmable optical quantum computer: the Borealis [17].

The current development in quantum computing is in a state that is hard to be surpassed by IBM in the U.S. IBM's Osprey outachieves a leading number of quantum bits in addition to its multi-level wiring, which provides flexibility in signal routing and device layout [15]. This cabling that separates the wires and other components required for readout and control onto their respective layers helps protect the fragile quantum bits from damage and helps the processor incorporate more quantum bits. Moreover, IBM has adopted a new type of flex wiring for low-temperature environments to help microwave signal transmission and has incorporated integrated filtering to reduce noise and improve stability. This new flex wiring increases the line density by 70% and reduces the price per line by 5 [18]. In the future, IBM will focus on the following: 1. they will incorporate error suppression and mitigation to help kernel developers manage quantum hardware noise and take further steps on the path to error correction. 2. they plan to introduce classical parallel quantum computing in 2023 to solve the scaling problem. These processors push the limits of what can be achieved with single-chip processors and control of large systems [19].

On the software level, NVIDIA is solving the MaxCut problem in 2021 using their latest creation using cuQuantum, a software development kit from NVIDIA that enables users to accelerate easily and scale quantum circuit simulations using GPUs. A natural tool for computing state vectors, it enables users to simulate quantum circuits that are deeper (more gates) and wider (more quantum bits) than today's quantum computers. And NVIDIA solved the MaxCut problem by running cuQuantum on their in-house supercomputer Selene, using 896 GPUs to emulate 1,688 quantum bits, capable of processing graphics containing up to 3,375 vertices. This is an 8-fold increase in quantum bits over previous mega-quantum simulations, as shown in Figure 3 below [20].

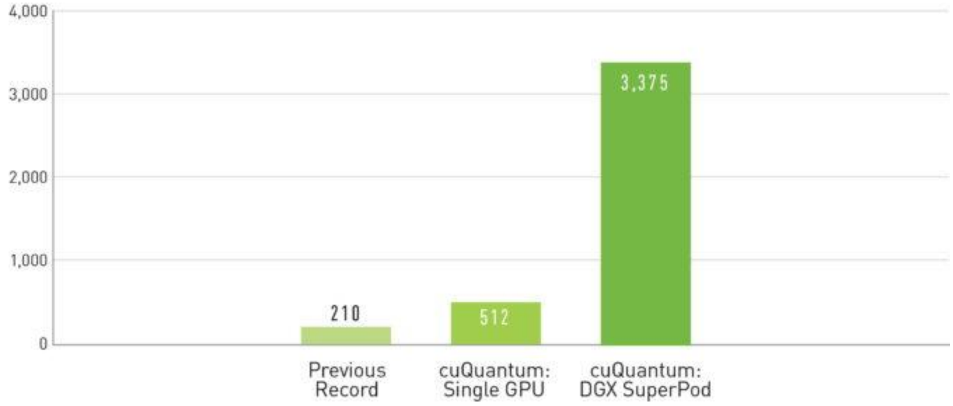

Figure 3. CuQuantum Performance Demonstration [20].

5. Conclusion

5.1. Summary and overview of the quantum computing field

The structure of quantum computing is introduced with the concept and origin of quantum computing. The research and development of quantum computing in cryptography, chemistry, and artificial intelligence are reviewed. The paper concludes at the end with a summary and comparison. Quantum computing has undergone decades of development and is now used in many fields, and has great advantages over classical computing in specific areas. Various properties of quantum bits make quantum computing very special. The reader can easily understand the development of quantum computing; the differences and advantages with classical computing; the applications in three fields; and the problems faced today and the future trends.

References

[1] Argonne National Laboratory, *Remembering Paul Benioff, renowned scientist and quantum computing pioneer*, 11-May-2022. [Online]. Available: https://www.anl.gov/article/remembering-paul-benioff-renowned-scientist-and-quantum-computing-pioneer. [Accessed: 20-Apr-2023].

[2] R. P. Feynman, "Quantum mechanical computers," *Optics News*, 01-Feb-1985. [Online]. Available: https://doi.org/10.1364/ON.11.2.000011. [Accessed: 20-Apr-2023].

[3] R. P. Feynman, "Simulating physics with computers - International Journal of Theoretical Physics," *SpringerLink*, 1982. [Online]. Available: https://link.springer.com/article/10.1007/BF02650179. [Accessed: 20-Apr-2023].

[4] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 1999. [Online]. Available: https://epubs.siam.org/doi/10.1137/S0036144598347011. [Accessed: 20-Apr-2023].

[5] Ivan Djordjevic, "Quantum Information Processing and quantum error correction," *ScienceDirect*, 2012. [Online]. Available: https://www.sciencedirect.com/book/9780123854919/quantum-information-processing-and-quantum-error-correction. [Accessed: 20-Apr-2023].

[6] arvindpdmn Preena Patel, "Qubit," *Devopedia*, 30-Jan-2022. [Online]. Available: https://devopedia.org/qubit. [Accessed: 20-Apr-2023].

[7] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *arXiv.org*, 25-Jan-1996. [Online]. Available: https://arxiv.org/abs/quant-ph/9508027. [Accessed: 20-Apr-2023].

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," *arXiv.org*, 19-Nov-1996. [Online]. Available: https://arxiv.org/abs/quant-ph/9605043. [Accessed: 20-Apr-2023].

[9] L. K. Grover, "Quantum mechanics helps in searching for a needle in a Haystack," *arXiv.org*, 17-Jul-1997. [Online]. Available: https://arxiv.org/abs/quant-ph/9706033. [Accessed: 20-Apr-2023].

[10] A. S. Gillis, "What is quantum key distribution (QKD) and how does it work?," *security*, 30-Nov-2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD. [Accessed: 20-Apr-2023].

[11] ID Quantique SA, “Quantum Key Distribution,” *ID Quantique*, 16-Jan-2023. [Online]. Available: https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/?utm_source=google_ads_search&utm_medium=cpc&gclid=CjwKCAjw_YShBhAiEiwAMomsEHQLvnZoTnjSCS62zKV-ZzMAaqpr1wRjEnqmQovUWdKgh5QZmlOJoxoCkoQQAvD_BwE. [Accessed: 20-Apr-2023].

[12] B. Yirka, "Google conducts largest chemical simulation on a quantum computer to date," *Phys.org*, 28-Aug-2020. [Online]. Available: https://phys.org/news/2020-08-google-largest-chemical-simulation-quantum.html. [Accessed: 20-Apr-2023].

[13] Xiao Yuan, "A quantum-computing advantage for chemistry | science," *A quantum-computing advantage for chemistry*, 28-Aug-2020. [Online]. Available: https://www.science.org/doi/10.1126/science.abd3880. [Accessed: 20-Apr-2023].

[14] TensorFlow, "Tensorflow Quantum," *TensorFlow*, 19-Dec-2022. [Online]. Available: https://www.tensorflow.org/quantum?hl=zh-cn. [Accessed: 20-Apr-2023].

[15] Hugh Collins and Chris Nay, "IBM unveils 400 qubit-plus quantum processor and next-generation IBM Quantum System Two," *IBM Newsroom*, 09-Nov-2022. [Online]. Available: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two. [Accessed: 20-Apr-2023].

[16] Kortny Rolston-Duce, "Quantinuum announces a world record in fidelity for quantum computing qubits," *Accelerating Quantum Computing*, 03-Mar-2022. [Online]. Available: https://www.quantinuum.com/news/quantinuum-announces-a-world-record-in-fidelity-for-quantum-computing-qubits. [Accessed: 20-Apr-2023].

[17] Lars S. Madsen, Fabian Laudenbach, and Mohsen Falamarzi. Askarani, "Quantum computational advantage with a programmable photonic processor," *Nature*, 2022. [Online]. Available: https://www.nature.com/articles/s41586-022-04725-x. [Accessed: 20-Apr-2023].

[18] J. Gambetta, "Quantum-centric supercomputing: The Next Wave of computing," *IBM Research Blog*, 22-Dec-2022. [Online]. Available: https://research.ibm.com/blog/next-wave-quantum-centric-supercomputing. [Accessed: 20-Apr-2023].

[19] IBM, "IBM Quantum Computing: Roadmap," *IBM Quantum Computing | Roadmap*, 01-Oct-2015. [Online]. Available: https://www.ibm.com/quantum/roadmap. [Accessed: 20-Apr-2023].

[20] S. Stanwyck, "Nvidia sets world record for quantum computing simulation with Cuquantum running on DGX superpod," *NVIDIA Blog*, 28-Apr-2022. [Online]. Available: https://blogs.nvidia.com/blog/2021/11/09/cuquantum-world-record/. [Accessed: 20-Apr-2023].