

Review of Quantum Computer Development

Kang Xiao

Shenzhen Ocahs International Academy, China

Abstract. In recent years, quantum computers have been attracting attention. Quantum computers have become a hot topic of research in today's scientific research. This paper first introduces the basic principles of quantum computers, including the storage principle and quantum logic gates, then introduces a quantum algorithm, then introduces the organization of quantum computers, and finally is a discussion that will evaluate the strengths and weaknesses of quantum computers, and discusses the physical implementation of quantum computers and the outlook on quantum computing.

Keywords: Quantum computing; quantum computers; quantum logic gates; quantum algorithms; physical implementation; outlook.

1. Introduction

In the information age, the increase in human demand for information has promoted a continuous commitment to information technology development. The creation of a new generation of high-performance and secure computing tools and communication technologies is a product of the combination of quantum theory and information theory. Quantum properties have unique functions in the field of information and may break the limits of existing classical information systems in terms of increasing computing speed, ensuring information security, increasing information capacity, and improving detection accuracy. With the rapid progress of interdisciplinary research between computer science and physics, theoretical and experimental research on quantum computing has flourished. Recent research advances have shown that the application of quantum information generation, loading, propagation, and processing may construct high-performance quantum computers. Quantum computers have become a hot topic of research in scientific research today.

2. The basic principle of the quantum computer

A quantum computer, as the name implies, is a machine that implements quantum computing. It is a class of physical devices that follow the quantum mechanical properties and laws of physical systems to perform high-speed mathematical and logical calculations, and store and process quantum information. When a device processes and computes quantum information and runs quantum algorithms, it is a quantum computer. A quantum computer follows unique laws of quantum dynamics (especially quantum interference) to implement a new paradigm of information processing. It uses atomic quantum states as memory units, switching circuits, and information storage forms. The various components that make up the hardware of a quantum computer reach atomic dimensions and are less than 1% of the size of similar components nowadays. For parallel processing of computational problems, quantum computers have an absolute speed advantage over classical computers. Quantum computers follow the basic principles of quantum mechanics: the discrete properties of quantum mechanical variables, the state iteration principle, and quantum coherence.

2.1. The storage principle of quantum computers

From the physical point of view, a computer is a physical system, and computation is the physical process by which this system evolves. Classical information systems use binary data bits to store data or programs, and each binary data bit is represented by a 0 or a 1, called a bit or bit (bit), as a unit of information. Macroscopic electronic computing uses a high or low potential to represent a 0 or a 1 for storage and computation. For example, the voltage between the poles of a capacitor is used to represent a bit of information, with a charge representing 1 and without a charge representing 0. In

quantum information systems, the data bits in a quantum computer can be constructed with spin or two-energy states, as distinct from classical computers, called quantum bits or qubits, to represent the unit of information. For example, the two polarization directions of photons $\leftarrow$ and $\rightarrow$, the two directions of electron spin or nuclear spin up and down in a magnetic field, and the two energy states of electrons in an atom. The process of quantum computing by a quantum computer is the evolution of the quantum states of these quantum mechanical systems. In a classical computer, each data bit is either a 0 or a 1, whichever is necessary. The bit string encoding using 0s and 1s characterizes different information, respectively. Unlike classical computer data bits, quantum bits can be either 0 or 1, or both 0 and 1. Operating on a quantum bit once is equivalent to operating on a classical bit twice. This is one of the advantages of quantum computing. For quantum computing, quantum bits are represented by two quantum states and the eigenstates $|0\rangle$ and $|1\rangle$, respectively, which are then encoded with the classical bits 0 and 1. A quantum bit can exist in such a state, neither $|0\rangle$ nor $|1\rangle$, and it can exist as a superposition of two logical states, i.e., $|X\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, α , and β are complex numbers. In a quantum computer, we cannot determine exactly which quantum state the quantum bit is in, i.e., we cannot determine the exact values of α and β . Quantum mechanics tells us that we can only get more and more information about this quantum bit and that the state of this quantum bit can be on any quantum state between $|0\rangle$ and $|1\rangle$, but it is impossible to determine its state completely. In other words, quantum computing includes all possible transformations. Therefore, the characteristics of quantum computers are.

(1) The input and output states of quantum computers are general superposition states, which are usually not orthogonal to each other;

(2) The transformations in the quantum computer are all possible transformations. After the output state is obtained, the quantum computer performs certain measurements on the output state and gives the calculation results.

It can be seen that quantum computing is a great expansion of classical computing. From another point of view, in the classical computer, a binary bit (bit) can only store a data, n binary bits can only store n a binary number or an n -bit binary number; while in the quantum computer, a quantum bit (qubit) can store two data, n quantum bits can store 2^n data at the same time, thus greatly improving the storage capacity.

2.2. Quantum logic gates

Computers consist of a network of memories and logic gates, but the storage contents and logic gates of quantum computers are different from those of classical computers. Just as a classical computer is based on a general-purpose Turing machine, a quantum computer can be based on a quantum Turing machine. Theoretically, it has been shown that a quantum Turing machine can be equated to a quantum logic circuit, and therefore a quantum computer can be constructed by combining some quantum logic gates. A quantum logic gate is the most basic operation on quantum bits. The basic logic gates in a classical computer are with and without gates. For quantum computers, it is known from quantum mechanics that all operations must be reversible, so the basic logic gates must also be reversible, but with gates are not reversible-the output and the input do not correspond to each other. If the output is 0, there is no way to determine whether the input is (0, 0), (0, 1), or (1, 0). Similarly, or-gate, hetero-or-gate, with-or-with gate, and non-gate are also irreversible. So in a quantum computer, with-gate, or-gate, opposite-or-gate, with- and non-gate and non-gate are not available. Using control non-gates and one-bit rotation operations, all reversible operations can be composed to achieve a wide variety of operations. Quantum logic gates can be classified into single-bit, two-bit, and three-bit logic gates according to the number of input bits. Because quantum logic gates are reversible, the number of input and output bits are equal. The quantum logic gate performs a deterministic least positive transformation on the input bits to obtain the output bits. Deutsch was the first to consider the problem of constructing computers with quantum logic gates, and he found that almost all three-bit quantum logic gates are universal. A universal logic gate means that a cascade of such gates can approximate any of the operations with arbitrary precision.

Many people later developed Deutsch's result and finally Deutsch and Lloyd each independently proved [1] that almost all two-bit quantum logic gates are universal. Moreover, since all quantum logic gates are reversible and are not accompanied by information erasure (loss of input information), there is theoretically no limit to thermal dissipation, thus eliminating the problem of thermal dissipation that fundamentally affects the normal function of the device, which cannot be solved by classical computers.

3. Quantum algorithms

Some specific quantum algorithms can be constructed by the basic quantum you-transform. Although the inputs, transformations, and outputs of quantum computing are very different from those of classical computing, quantum algorithms with higher efficacy than classical algorithms can be constructed by rational construction of the you-transformations (quantum gates) and measurement timing.

Many problems with high computational complexity (e.g., NP problems) often cannot be efficiently computed on classical computers, and due to the quantum parallelism principle of quantum computing, the computational power can be accelerated exponentially compared to classical computing. It is not yet possible to prove whether P problems and NP problems belong to the same complexity class (i.e., $P \neq NP$), and most people believe that P is for NP . For quantum computing, if NP is indeed not a P problem, then quantum computing is likely to be much more capable than classical computing, which is possible evidence that quantum computing surpasses classical computing.

Quantum computing must have efficient quantum algorithms to exploit its computational advantages, and there has been much research on quantum algorithms [2-9]. In the principle of parallelism, although it is possible to produce all computational results by only one transformation, however, only one result can be obtained when measuring and the desired result cannot be selected. The central idea of quantum algorithms is to exploit the coherence (coherence) of quantum states so that the objectively desired result is enhanced while the undesired result is weakened so that the objectively desired result appears with a fairly high probability at the time of measurement.

Find a series of prime factors of a large number N such that the multiplication is equal to N . This is a problem of exponential complexity, and the most efficient classical algorithm so far (sieve method)

has a time complexity of $O(e^{n^{\frac{1}{3}} \lg^{\frac{2}{3}} n})$ [10], which is computationally very impressive if N is large. If N is a 250-bit integer (decimal), it is estimated to take about 800,000 years to compute collaboratively with 1600 workstations. The difficulty of large number prime factorization is the theoretical basis for the security of the well-known RSA public key system, which is now widely used in electronic banking, network security, and other fields.

In 1994, Shor proposed a quantum algorithm for the factorization of large numbers[2], where the upper bound on the time complexity of finding two prime factors of an n -bit (binary bit) large number is $O(n^2(\lg n)(\lg \lg n))$, which is a polynomial in n (with a wider upper bound of $O(n^3)$) is computed on a quantum computer. Thus, Shor's algorithm transforms the large number factorization, a super-polynomial time complexity problem on a classical computer, into a polynomial time complexity problem on a quantum computer. This result suggests that a large number of keys can be cracked in polynomial time using future quantum computers, challenging the security of the RSA public key system.

The basic idea of Shor's algorithm is to first obtain all the function values by one-step computation using quantum parallelism, and then obtain the superposition states of the associated function independent variables by measuring the functions and performing Quantum Fast Fourier Transformation(QFFT) on them. The QFFT is also used to transform the decomposition of large prime factors into the problem of finding the period of a function in polynomial steps. Let N be the large integer to be decomposed, first choose a natural number c randomly with N mutually prime, and construct the function: $f(x)=c^x(\text{mod}N)$. Shor proves that by finding the period of the function $f(x)$,

a factorization of N can be obtained according to a certain procedure[2]. Finding the period of $f(x)$ uses the QFFT algorithm: if there is a quantum bit input state $|\Psi_i\rangle = \sum_{x=000\dots 0}^{111\dots 1} f(x)|x\rangle$, its QFFT is

$$|\Psi_i\rangle = \sum_{x=000\dots 0}^{111\dots 1} [2^{-\frac{k}{2}} \sum e^{2\pi i x x'}] f(x')|x\rangle, \text{ where } k \text{ is the data length of } x \text{ in binary representation. It can be}$$

seen that the QFFT is a discrete Fourier transform that changes the superposition coefficients in front of the quantum state into the original superposition coefficients. It can be shown that the above change can be done in approximately k^2 steps (with time complexity of about $O(n^2)$). The period of the original superposition coefficients can be obtained by measuring the phase of the transformed wave function. Once the period of $f(x)$ is obtained, a factorization of N can be derived according to a certain probabilistic algorithm, but since it is a probabilistic algorithm, it may not succeed every time. Shor proved that the probability of success in solving the calculation decreases only polynomially with the binary length of the input data N [11]. Thus, by repeating the above procedure polynomial times, a factor of N can be found with a probability very close to 1. A polynomial algorithm with polynomial times repetition is still a polynomial algorithm[9].

In terms of fast search of databases, for example, finding a particular element in a table with 25 elements takes on average 12-13 attempts to succeed with a classical computer, and in the worst case 25 attempts. In 1996 Grover of AT&T Bell Labs proposed Grover's algorithm, proving that the number of searches required to perform the above search with a quantum computer does not exceed 5. In general, for a database of N elements, it takes an average of 2 attempts to step to succeed with a classical computer, while a quantum computer supplemented with Grover's algorithm does not require more than $\sqrt{N}$. The superiority of speed is evident at large N . This is because the quantum computer superimposes the N searched objects of the database as 1 state in Hilbert space, and the state to be searched is only one component of it[3].

4. The architecture of quantum computers

A quantum computer is a device that performs quantum computation, and its computation process is determined by algorithms, and different algorithms have different You-transformations. The computational process of a quantum computer is consistent with the execution process of a quantum program, as shown in Figure 1, where $U_i = 1, 2, \dots, n$ are all You-transformations[12].

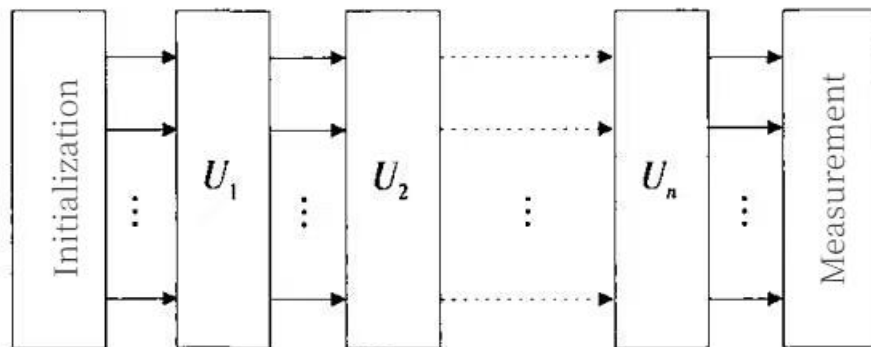


Figure. 1 Computational process of the quantum computer

It is generally believed that the physical entity of a quantum computer should consist of two parts: the quantum part and the classical part. Since the effectiveness of quantum computing is mainly shown by the powerful processing of data, it is generally preferred that the quantum part should handle the data while the classical part should handle the control. That is, a classical computer is used to control the quantum devices to operate on quantum bits. Such an organization takes into account mainly the engineering problems of quantum computer implementation (the difficulty of joint

participation of multiple quantum bits in control and computation). A simple control schematic of a quantum computer is given in Figure 2[12]. Since the measurements of quantum computing are probabilistic, they need to be calculated and premeasured several times to obtain the desired results.

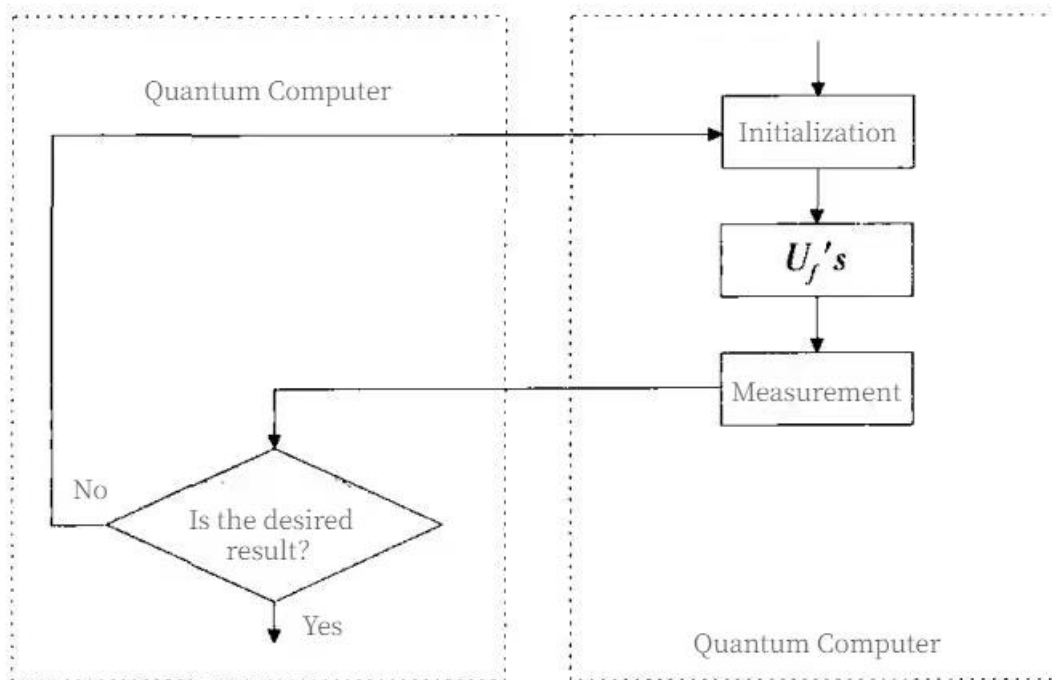


Figure. 2 Control of a quantum computer

As can be seen in Figure 2, the interaction of information between the classical computer and the quantum computer is required before the start and after the end of the calculation, and at these two moments, since the state of the quantum bits in the quantum computer is in a stable ground state (or has not yet formed a superposition state, or has collapsed past the measurement), such an organization does not destroy the closed nature of the quantum computer.

Quantum parallelism is a characteristic of quantum computers, which do not have advantages for serial computing[12]. Until the emergence of general-purpose quantum computers, quantum computers are suitable as high-speed co-processors or peripheral special processors of classical general-purpose computers, or special computers dedicated to the implementation of some quantum algorithm or the simulation of some quantum system. The quantum computers currently studied are in principle dedicated processors attached to a classical general-purpose computer, and its programming language is a general-purpose computer programming language with some components to support quantum computing[12-13].

5. Advantages and Disadvantages of Quantum Computers

5.1. Advantages over traditional computers

The operation speed of conventional computers can only be guaranteed at a certain temperature, and the heat dissipation of computer chips will reduce the computing speed. It was found that the irreversible operation in the computing process is the main cause of high energy consumption, and the most prominent advantage of quantum computers is the ability to perform reversible operations, which solves the energy consumption problem that is difficult to avoid in traditional computing into. According to Moore's law, the performance of integrated circuits can double every 18-24 months, and the price will drop to 0.5 times the original price when the cost of materials and technology remains the same. By this law, we can feel the rapid progress of information technology, but one day will reach the limits of this law. The wiring density of computer chips is a great limiting reason, once it reaches a certain limit density, it will no longer follow Moore's law, at this time the wave-particle

duality can not be ignored, according to the Heisenberg uncertainty relationship, the uncertainty of electron position is very small, the uncertainty of momentum will be large, the quantum effect is significant, precise operation of the electron is extremely difficult, easy to cause component failure. Therefore the integration of the components is limited, and the unit volume of computing speed has been greatly affected, but the quantum computer can well overcome this point.

5.2. Quantum computer experimental difficulties

5.2.1 Quantum decoherence

Coherence in quantum computing is the essence of quantum parallel computing, but in practice, quantum bits are subject to the action and influence of the external environment, resulting in quantum entanglement. Quantum coherence is highly susceptible to the interference of quantum entanglement, which leads to the reduction of quantum coherence, also known as the decoherence phenomenon. In practical applications, it is impossible to avoid the contact between quantum bits and the outside world, and the quantum coherence is not easily maintained. Therefore, the quantum decoherence problem is one of the important problems that need to be solved at present, and its solution will affect the future development path of quantum computers to a certain extent.

5.2.2 Quantum entanglement

Quantum, as the smallest particle, obeys the law of quantum entanglement. Even though the quanta may be separated from each other in space, the interaction between the quanta is unavoidable. In between, quantum entanglement technology is associated with the field of quantum information transfer. In a certain sense, the fast communication speed between quanta is used to transmit information.

5.2.3 Quantum Parallel Computing

The unique parallel computing of quantum computers is an important point that cannot be matched by classical computers. Also an n -bit memory, classical computers store only one result.

But quantum computers store results up to $2n$. Their parallel computing not only far surpasses the latter in terms of storage capacity, but also in terms of reading speed, and multiple reads and calculations can be performed simultaneously. It is important for quantum parallel computing and its effective application has become one of the keys to the development of quantum computers.

5.2.4 Quantum unclonable

Quantum unclonability means that there is no process of replication of any unknown quantum state, and since the quantum state has to be kept unchanged, there is no measurement of the quantum, and no replication can be achieved. For quantum computers, the error correction applications of classical computers, as well as the replication function, cannot be realized.

6. The physical implementation of quantum computers

The composition of a quantum computer has to involve many theoretical and technical aspects such as quantum bits, quantum logic gates, quantum wires, quantum ciphers, etc. It also has to involve the principle of state superposition, two-energy systems (or two-state systems), entangled states, density matrices, information entropy, and many other basic concepts of quantum mechanics. Therefore there are many obvious problems in studying quantum computers. It is indeed too difficult to experimentally implement the manipulation of microscopic quantum states. First of all, there is the decoherence problem. The most essential difference between quantum computers and classical machines is that the former exploits quantum coherence to achieve quantum parallel operations, while quantum systems in superposition or entanglement states can decoherence due to inevitable noise so that the normal coherent evolution suffers from disruptions and computational errors. Thus, how to correct errors is also a major research topic for quantum computers. Research in quantum computing has greatly simplified the physical implementation of quantum computers.

With quantum logic gates and quantum bits to store information, it is possible to build quantum computers. Since the controlled rotation between two quantum bits is sufficient to construct arbitrarily complex quantum computing networks, the most fundamental logical component of a quantum computer is a controlled physical system of two quantum bits, so that the interactions between them can evolve according to the state conditions of one bit to the other. Such physical systems have been proposed for cavity quantum electrodynamics, quantum dots in semiconductors, photonic lattices, multiplexed pulsed magnetic resonance, and supercooled ions. The key to realizing quantum computing is to realize controlled non-gates to complete the logic operation between quantum bits, and the latter two schemes have strong feasibility.

In 2000, Hitachi, Japan, developed a successful quantum component - "single electron transistor", which can control the movement of a single electron and has the characteristics of small size and low power consumption, about 1000 times lower than the current power consumption of the smallest transistor. Trillions of transistors can be accommodated on a small chip, making the integration of integrated circuits much higher.

In 2001, scientists at IBM constructed a 7-bit nuclear magnetic resonance (NMR) quantum computer. IBM's experiment turns an atom into an ion and uses two internal spin states of the ion as a qubit, and then uses a microwave pulse as the address. This quantum computer, built by using NMR techniques to measure and control the spin of a single atom, uses pulses of radio waves to enable the computer to begin computational processing by changing the atomic energy level so that the atom interacts with other atoms in a controlled manner.

In September 2004, NTT's Institute for Fundamental Research in Physical Sciences (IFPBS) piloted the development of a "superconducting magnetic beam quantum bit", the most promising basic component of a quantum computer. Compared with other basic units, the superconducting magnetic beam quantum bit has the advantages of easy and continuous maintenance of quantum state and easy integration. This makes it possible to realize quantum entanglement using multiple components to process multiple pieces of information simultaneously, and thus to realize control non-gates that constitute a basic circuit, etc. This time, it is microwaved, which has lower energy than light, that is used for bit control but can still control the amplitude of energy jumps well, thus opening the way for applications in optical control as well. By combining optical communication with the unit developed here, e.g., through a fiber optic network, a collaboration between quantum computers can be achieved.

Currently, experimental physicists are searching for more efficient preparation paths to overcome decoherence and achieve cascading of logic gates. Although various quantum error correction codes have been proposed theoretically, it is still a challenging problem to use quantum coding to overcome the decoherence effectively in experiments.

7. Outlook

Today, with the rapid development of technology, the powerful computing power of quantum computers will be applied to various fields and will herald the arrival of a new situation in the computer world. The emerging industry of quantum computers will certainly have an important position in the future computer field. The gradual improvement of the AI industry level nowadays has set off the world AI boom. The supercomputing power of quantum computers is expected to accelerate the process of the AI industry and promote the rapid development of the AI industry in the future. Quantum computing is nowadays mainly used for complex large-scale data processing, and network security services based on quantum encryption. While AI is becoming more demanding in terms of computing power, quantum computing can provide its supercomputing power for this purpose. High-speed parallel computing through its core strengths.

With the gradual improvement of the technology, it will also become a possibility in the field involving molecular modeling, i.e., the accurate simulation of intermolecular interactions after the optimal configuration of chemical reactions. Currently, classical computers can only analyze the

simplest of molecules, quantum computers can make a comprehensive analysis of complex chemical reactions through their efficient computing power. Google has already produced the first quantum simulation of a hydrogen molecule in this field, and if we use this method to apply to more molecules and other substances, it will involve many fields around us, from new energy to the development of drugs. This is something that has not been achieved by traditional means. It is clear that with the development of quantum computers, more efficient products will appear in our lives.

References

- [1] Turing A M. On computable numbers, with an application to the Entscheidungs problem [C]//Proc Lond Math Soc 2, 1936,42:230-265.
- [2] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring [M]. New Mexico: IEEE Computer Society Press, 1994:124-134.
- [3] Grover L K. A fast quantum mechanical algorithm for database search. 1996:212-219.
- [4] Hoyer P. Efficient quantum transforms. arXiv , quant-ph/ 9702028,1997.
- [5] Collins D, Kim K W, Holton W C. Deutsch-Jozsa algorithm as a test of quantum computation[J]. Physical Review A, 1998,58(3) : 1633-1636.
- [6] Cleve R, Ekert A, Macchiavello C. Quantum algorithms re-visited [C]//Proc Roy Soc London A , 1998,454 (1969): 339-354.
- [7] Cleve R, Ekert A, Henderson H. On quantum algorithm. arXiv , quant-ph/9903061,1999.
- [8] Hoyer P. Conjugated operations in quantum algorithms[J]. Physical Review A, 1999,59(5): 3280-3289.
- [9] Shor P W. Introduction to quantum algorithms. arXiv, quant-ph/0005003,2000.
- [10] Lenstra A K, Lenstra H W. The development of the number field sieve[M]. Berlin : Springer-Verlag, 1993.
- [11] Shor P. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J on Computing, 1997,26: 1484-1509.
- [12] Xia P S. Quantum computing[J] Journal of Computer Research and Development,2001,38(10): 1153-1171.
- [13] Omer B. Structured quantum programming [D]. Institute for Theoretical Physics, Technical University of Vienna,2003.
- [14] Wang Y., Huang D. C., Yu Y. H. Advances in quantum computing and quantum algorithms [J]. Computer Systems Applications,2011,20(06):228-231+237.
- [15] Wang Shuhao, Long Guilu. Big data and quantum computing [J]. Science Bulletin,2015,60(Z1): 499-508.
- [16] Huanguo Zhang, Shaowu Mao, Wanqing Wu, Shuomei Wu, Jinhui Liu, Houzhen Wang, Jianwei Jia. A review of quantum computing complexity theory [J]. Journal of Computer Science,2016,39(12):2403-2428.
- [17] Yao QZ. The last kilometer to quantum computing [N]. China Information Technology Weekly, 2017-11-13(007).
- [18] Wang Bangchun. Quantum computing cloud platform released [N]. China High-Tech Industry Herald, 2017-10-16(003).
- [19] CAS Institute of Quantum Innovation and Aliyun release a quantum computing cloud platform [J]. Electronic World,2017,(20):200.