Principles and Characteristics of Quantum Computing

Dianhao Liu

College of Nuclear Equipment and Nuclear Engineering, Yantai University, Yantai 264005, China

*Corresponding author’s e-mail: ldh0510@163.com

Abstract. With the rapid development of science and technology, people tend to have a higher demand for computing. Classical computers can no longer meet part of the computing needs, so quantum information systems have gained more and more attention. Quantum computers have good parallelism, fast information processing speed, large amount of information storage, and performance in many fields far surpasses classical computers. In this article, the author introduces coherent superposition and part of quantum gates and quantum algorithms meanwhile compares classical computers with quantum computers in many aspects. The advantages and disadvantages of quantum computers in principle are also drawn out. Finally, the author proposes future prospects for quantum computers prediction.

1. Introduction

With the advancement of science and technology, mankind has entered the information age. Classical computers that are based on circuits have been widely used. Scientific research, military, economics, and life become increasingly dependent on computers. With the establishment and improvement of quantum mechanics, many fields that are combined with quantum mechanics and breakthroughs have been made. Some properties of quantum mechanics are suitable for information processing. Thus, the interdisciplinary subject of quantum mechanics and existing information technology was born, which is called quantum informatics. Quantum computer is a part of quantum informatics. It surpasses classical computers in terms of the speed of parallel operation, the efficiency of information storage and the security of information encryption. Some differences in principle make the performance of quantum computers in certain fields easily surpass classical computers. This makes multiple systems such as encryption systems and information transmission, based on classic computers, a challenging position. Quantum informatics has good development prospects, and has been valued by research institutions, governments, enterprises and the armed forces. In this article, the author will introduce qubits, basic quantum gates and some quantum algorithms, as well as discuss the advantages and disadvantages of quantum computers and the future development prospects of quantum computers [1].

2. Overview of quantum bit

In the classic method, a bit is used as an information unit, and a bit can only be one of the two states of 0 or 1. Traditional bits are stored on the capacitor plate in the form of voltage. In a quantum information system, the information unit is a qubit. Qubits are similar to two-state systems such as half-spin or two-level atoms. Due to quantum superposition, the basic state of a qubit can be not only |0> or |1>, but also |ψ>=a|0>+b|1> (the linear superposition state of |0> and |1>). An n-bit classical
register can only store one of $2^n$ numbers, while an n-bit quantum register has $2^n$ mutually orthogonal quantum states, it can store the superposition of all $2^n$ states [2,3].

3. Hardware of quantum computing

Josephson junction (see figure 1) is the hardware foundation of quantum computing. In the structure of Josephson junction, a very thin (usually 10A) insulator is placed between the two superconductors. This structure forms a potential energy barrier. In superconductors, atoms near the Fermi surface attract each other, forming many Cooper pairs. These Cooper pairs pass through the insulator layer and move between the two superconductor layers due to the tunneling effect [4].

![Figure 1. Josephson junction](image)

When the voltage across the Josephson junction is zero, there is superconducting current. The superconducting current has a theoretical maximum $I_c$, but it is greatly affected by the external magnetic field, so $I_x$ is smaller than $I_c$. This is the first formula of Josephson.

$$I_x = I_c \sin \psi$$  \hspace{1cm} (1)

When the voltage across the Josephson junction is not zero, there is still a superconductor pair tunneling current, but this circuit is an alternating superconducting current, and its frequency is proportional to $f$ and $V_0$. The characteristics of this current are summarized as Josephson's second formula.

$$\frac{d\psi}{dt} = \frac{2eV_0}{h}$$  \hspace{1cm} (2)

According to Josephson's first and second formulas, the equivalent inductance of the Josephson junction can be obtained.

$$L = \frac{\Phi_0}{2\pi I_c \cos \psi}$$  \hspace{1cm} (3)

In this formula $\Phi_0 = \frac{h}{2e}$, which is the magnetic flux quantum. This formula shows that the inductance of the Josephson junction is non-linear, and the inductance will change as $\psi$ change. Although the energy level of the circuit constructed by Josephson is similar to that of the resonator, the energy level interval is not the same. This feature can effectively separate the 0 and 1 energy levels from other energy levels, and it is very important for the construction of qubits [5].

4. Quantum logic gates

Similar to classical logic gates for classical signals, quantum logic gates (or called quantum gates) are used to process quantum signals and form quantum computing systems. Unlike classical logic gates, quantum logic gates are reversible and will not lose input signals. Moreover, quantum logics do not have heat dissipation problems, which fundamentally avoids the problem of classical logic gates, which is unable to operate normally due to insufficient heat dissipation. According to the number of input qubits, quantum logic gates are divided into single-qubit gates and multi-qubit gates. The basic
quantum logic gates constitute complex metric logic gates, and these logic gates constitute the entire quantum information system [6].

4.1. Pauli gate
X gate, Y gate and Z gate correspond to Pauli matrix X, Y, Z respectively.

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} 
\]

(4)

\[
Y = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} 
\]

(5)

\[
Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} 
\]

(6)

It is equivalent to rotating 180 on the corresponding coordinate axis on the Bloch sphere. The x gate in the quantum gate is similar to the NOT gate in the classical logic gate.

4.2. Hadamard gate
The Hadamard gate is a single qubit gate, it corresponds to the matrix H.

\[
H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} 
\]

(7)

The function of this gate is to transform \(|0>\) into \(|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\) and transform \(|1>\) into \(|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\). This logic gate is actually a Hilbert space transformation, from the eigenvectors \(|0>\) and \(|1>\) of the Pauli Z matrix to the eigenvectors \(|+\rangle\) and \(|-\rangle\) of the Pauli X matrix.

4.3. Phase shift gate
The phase shift gate is a quantum gate that operates on a single qubit, it corresponds to the matrix S.

\[
S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} 
\]

(8)

The function of this gate is transform \(|1>\) into \(|e^{i\theta} >\) and not change \(|0>\). \([a|0>+b|1>\] will become \([a|0> +e^{i\theta} b|1>\] after being processed by this quantum gate. It is equivalent to rotating \(\theta\) degrees on the Bloch sphere.

4.4. \(\pi/8\) gate
The phase shift gate with \(\theta = \pi/8\) is called \(\pi/8\) gate, it is a special kind of phase shift gate and it corresponds to the matrix T.

\[
T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\pi/4} \\ e^{-i\pi/4} & 1 \end{pmatrix} 
\]

(9)

This quantum gate changes the input \([a|0> + b|1>\] into \([a|0> + e^{i\pi/4} b|1>\] as output. It is equivalent to rotating \(\theta\) degrees on the Bloch sphere.

4.5. CNOT gate
The CNOT gate, which can been in figure 2, is a multi-qubit gate, it corresponds to matrix CNOT.

\[
\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} 
\]

(10)

The function of this gate does not change the control qubit, but performs an exclusive XOR operation on the controlled qubit (when the control qubit is 0, the controlled qubit is not changed. When the control qubit is 1, the control qubit is Bit perform not operation).
4.6. **SWAP gate**
The SWAP gate is a multi-qubit gate, it corresponds to matrix SWAP.

\[
\text{SWAP} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

The function of this gate is to exchange two input qubits. The SWAP gate is composed of three CNOT gates. When \(|a, b>\) passes through the first gate, the information is changed to \(|a, a \oplus b>\). The second gate converts the output of the previous gate to \(|a \oplus (a \oplus b), a \oplus b> = |b, a \oplus b>\). The information processed by the second gate is turned into \(|b, (a \oplus b) \oplus b> = |b, a>\) by the third gate. Through these processes, the two input signals are exchanged (see figure 3 and figure 4) [7].

5. **Quantum algorithm**
Quantum algorithm is an algorithm used in quantum computing. This algorithm uses the characteristics of quantum mechanics to operate, and it has huge advantages over classical algorithms in many aspects.

5.1. **Shor's algorithm**
Shor's algorithm is a very effective quantum algorithm, mainly used for factorization of large numbers. Factorization of large numbers is applied to RSA public-key cryptosystem, which is an encryption algorithm used in many banks and online accounts. Shor's algorithm can convert the factorization of large numbers into calculating the period of a function. The calculation speed of a quantum computer is much faster than that of a classical computer when calculating the period. The Shor algorithm
makes it possible to crack the RSA public-key cryptosystem, and the security of banks and websites using RSA will be challenged [8].

5.2. **Grover’s algorithm**

Grover's algorithm is another highly efficient quantum algorithm, called a quantum search algorithm. This algorithm is very suitable for finding a data from many unordered data. The time complexity of the classic algorithm is $O(N)$, while the time complexity of Grover's algorithm is $O(\sqrt{N})$. This means that when solving the same problem, choosing Grover's algorithm to solve it will save a lot of time than choosing the classic algorithm. The Grover algorithm has a wide range of uses, and can be applied to mathematical calculations, password cracking, nuclear magnetic resonance, optics, and so on [9].

6. **Advantages and disadvantages of quantum computing**

6.1. **Advantages of quantum computing**

Firstly, quantum computers have natural parallelism, which can handle a problem in simple steps, which will be difficult to calculate when using classical computers. This kind of parallelism brings about a reduction in time complexity, leading to a wide range of applications of quantum computers in many fields, and may even affect the future development of certain fields.

Secondly, quantum computers have applications in many fields. It can be used to crack codes, which will affect finance and military affairs. It can also be used to solve mathematical problems. The high efficiency of quantum computers in certain aspects will make some unsolvable mathematical problems possible.

Thirdly, compared to classic bits, qubits can be used to store and compute more information. Under the same conditions, qubits can save more time and space.[10]

6.2. **Disadvantages of quantum computing**

At first, the quantum computer can process the quantum of the superposition state in parallel, and the superposition state of many results is obtained after the processing. This superposition state requires further observations to obtain a definite state, and observations will cause the wave function to collapse and cannot be measured again. In other words, only one result can be obtained in one operation, and problems with multiple solutions require multiple operations. This leads to fundamental flaws in quantum computers in dealing with problems that have multiple solutions.

Next, in the classic information storage method, 1 bit of information can only be 0 or 1, and this method has a relatively high error tolerance rate. Quantum information storage requires the superposition state of information $|0\rangle$ and $|1\rangle$ stored in 1 qubit. Some superposition states have very little difference. Quantum information storage requires a high degree of precision for the operation of quantum computers.

Lastly, classical information storage stores information in the form of voltage, and the information stored in this way changes little over time. The quantum memory stores coherent superimposed particles, but these particles will be decoherent over time, which means that the probability of information distortion is relatively high.

7. **Conclusion**

The author believes that quantum computers will have a very good development prospect. After a certain period of development, quantum computers will largely replace non-civilian classical computers. When the development of quantum computer becomes more mature, many fields will be replaced by it, which will force people to find a more secure encryption system. It will provide great help to research, and bring another way to the development of artificial intelligence. The problem facing quantum computing is to reduce and overcome the effects of quantum dissipation and quantum
decoherence, to find a more suitable physical system for quantum computers, and to effectively extract information from quantum systems.

8. References
[1] National Academies of Sciences, Engineering, and Medicine, Quantum computing: progress and prospects 2018 Washington DC: National Academies Press doi: 10.17226/25196
[2] Feynman R P 1982 Simulating physics with computers Int J Theor Phys 21( 6& 7) pp 467-488
[3] Steane A 1997 Quantum computing
[4] Yu X and Lu X and Xi J and Shao P N 2018 Overview of the progress of superconducting quantum chips based on Josephson junctions [J] Computer Engineering 44(12) pp 33-38+45
[5] Mao G F and Yu Y 2007 Superconducting qubits based on Josephson devices [J] Progress in Physics 01 pp 34-42
[6] Zhang D Y and Tan Y K 2019 Classical logic gates and quantum logic gates [J] Journal of Hengyang Normal University 40(03) pp 16-23
[7] Xia P S 2001 Quantum Computing [J] Computer Research and Development, 10 pp 1153-1171
[8] Samuel J and Lomonaco Jr 2002 Shor’s Quantum Factoring Algorithm. Proceedings of symposium in Applied Mathematics 58 pp 161-180
[9] Wu N and Song F M 2007 Quantum computing and quantum computers [J] Computer Science and Exploration 01 pp 1-16
[10] Guo G C and Zhang H and Wang Q 2017 Overview of Quantum Information Technology Development [J] Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition) 37(03) pp 1-14

Acknowledgments
First and foremost, I would like to show my deepest gratitude to my teachers and professors in my university, who have provided me with valuable guidance in every stage of the writing of this thesis. Further, I would like to thank my friends and parents for their encouragement and support. Without all their enlightening instruction and impressive kindness, I could not have completed my thesis.