

Research progress on quantum informatics and quantum computation

Yusheng Zhao¹

college of arts and science, New York university, New York 10012, US

Yz2188@nyu.edu

Abstract. Quantum informatics is an emerging interdisciplinary subject developed by the combination of quantum mechanics, information science, and computer science in the 1980s. The birth and development of quantum information science has far-reaching significance in science and technology.

At present, the application of quantum information technology has become the direction of people's efforts. The preparation, storage, purification and regulation, transmission, quantum coding and decoding of quantum state have become the hotspot of scientists and technicians, which have a profound impact on the national economy and the people's livelihood, technology and defense technology. This paper first summarizes the background of quantum information science and quantum computer and the current situation of domestic and foreign research, and then introduces the basic knowledge and basic concepts of quantum computing. Finally, several quantum algorithms are introduced in detail, including Quantum Fourier transform, Deutsch-Jozsa algorithm, Shor's quantum algorithm, quantum phase estimation.

1. Introduction

Quantum informatics mainly consists of quantum communication and quantum computation. Quantum information is based on the basic principles of quantum mechanics to deal with the information, the classic information is expanded to quantum information, and micro-system quantum state is used to express information, which makes quantum information science have many advantages the classical information does not possess, such as absolute security and confidential communication, ultra-fast computing and large capacity storage. The emergence and development of quantum information theory have far-reaching significance [1].

Quantum mechanics, information theory and computer science have experienced a long and complicated process from the initial parallel development to cross fusion. The generation of quantum mechanics dates back to the energy quantization proposed by Planck's epoch-making essay "On the law of distribution of energy in the normal spectrum" in 1900, through the efforts of physicists such as Einstein, Born, Dirac, quantum mechanics theory was officially founded. Of course, Einstein and Bohr as the representative of the two sides on the basic issues of quantum mechanics had severe debate, which has played a huge role in promoting the development of quantum mechanics. The creation of quantum mechanics has become an important part of science, and quickly applied to basic particles, atoms and molecules, solid and other different physical systems, which has achieved great success [2].

The real concept of quantum computer was first proposed by Feynman in combination with quantum mechanics and computer science in the 1980s. Later, Benioff proposed the quantum Turing machine. In 1985, Deutsch in his paper "Quantum theory, the Church-Turing principle and the universal quantum computer", according to the superposition of quantum states, he explained the principle of quantum Turing machine which can complete the parallel computing. In 1992, Brassard



and Berthiaume theoretically proved that the quantum Turing machine was faster than the classic Turing machine. But these development processes were still slow, and quantum computers were not being given enough attention. In 1994, Shor proposed a large number factor factorization algorithm, the Shor algorithm, based on the Quantum Fourier transform, which fully demonstrated the superiority of the quantum algorithm and rose the public RSA key system a great challenge, by that time, the value of quantum computer was able to be re-understood. Then, in 1995, Shor offered the first quantum error-correcting code in the history, as known as the Shor code. Steane gave the $[[7,1,3]]$ error code in 1996, confirming the existence of quantum code error code and tolerance code, which further proved the feasibility of quantum computing [3].

This paper mainly summarizes the basic knowledge and basic concepts of quantum computing, as well as several quantum algorithms in detail, including Quantum Fourier transform, Deutsch-Jozsa algorithm, Shor's quantum algorithm, quantum phase estimation and so on.

2. The Basic Assumptions of Quantum Mechanics

Quantum information theory is based on quantum mechanics, and quantum computing is a major branch of quantum information. The description of quantum computing is based on four basic assumptions: [1,4-5]

The physical state of the microscopic system is described by a vector of Hilbert space. The two vectors with a plural factor difference describe the same state.

The physical quantity of the microscopic system is described by the Hermitian operator in the Hilbert space. The value that the physical quantity can take is the eigenvalue of the corresponding operator. The physical quantity A takes the probability of each value a_i in the state $|\psi\rangle$, and the state vector $|\psi\rangle$ is proportional to the normalized eigenvector $\{|a_i\rangle\}$ of A , and the complex square of the coefficients of $|a_i\rangle$ in the expansion. Hence it is proportional to the complex square of c_i in the following formula:

$$|\psi\rangle = \sum_i c_i |a_i\rangle, c_i = \langle a_i | \psi \rangle,$$

The changing law over time of state $|\psi(t)\rangle$ of the microscopic system is described by the Schrodinger equation.

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = H |\psi(t)\rangle$$

Measure and collapse: Assuming that the system is in the superposition state $c_1|a_1\rangle + c_2|a_2\rangle$ of the eigenstates $|a_1\rangle$ and $|a_2\rangle$ of the mechanical quantity A , the mechanical quantities A are measured to obtain the results a_1 and a_2 with the probability of $|c_1|^2$ and $|c_2|^2$. Then, once the results are determined, the state of the system is determined as $|a_1\rangle$ or $|a_2\rangle$ rather than the superposition of both.

3. Quantum Logic Gate

In quantum computers, the basic unit of information is quantum bits, and the basic operation of information is quantum logic gates. Quantum bits are the carriers of information. Quantum bit information is processed by quantum logic gate, and finally the result is obtained.

Quantum information processing is a series of unitary evolution of the encoded quantum state. The quantum logic gate is the most basic unitary operation of the quantum bit. Unitarity is the only requirement of the quantum logic gate, and any matrix satisfying the unitary state can characterize a quantum logic gate. All quantum logic gates are operable, without the erasure of information (loss of input information), and there is no theoretical limit of heat dissipation.

Common quantum logic gates have single-bit revolving gates and two-bit quantum controlled not gate. The single-bit revolving door can be expressed as [6,7]:

$$\begin{aligned}
|0\rangle &\xrightarrow{R(\theta)} \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \\
|1\rangle &\xrightarrow{R(\theta)} \cos\frac{\theta}{2}|1\rangle + \sin\frac{\theta}{2}|0\rangle,
\end{aligned}$$

Where, θ is the angle of rotation.

Quantum controlled non-gate refers to a two-bit control gate (one bit as a controlling bit and the other as a controlled bit). The controlling bits remain constant during the logical operation, but its state determines the evolution of the controlled bits. If the controlling bit state is $|0\rangle$, then the controlled bit state does not change; if the controlling bit state is $|1\rangle$, then the controlled bit will be reversed. Quantum controlled-not gate can be expressed as (the first quantum state is the controlling bit; the second quantum state is the controlled bit) [8]:

$$\begin{aligned}
|0\rangle_1|0\rangle_2 &\rightarrow |0\rangle_1|0\rangle_2, & |0\rangle_1|1\rangle_2 &\rightarrow |0\rangle_1|1\rangle_2 \\
|1\rangle_1|0\rangle_2 &\rightarrow |1\rangle_1|1\rangle_2, & |1\rangle_1|1\rangle_2 &\rightarrow |1\rangle_1|0\rangle_2
\end{aligned}$$

The results show that single-bit revolving gates and two-bit quantum controlled gates can be combined to achieve any of the functions of quantum gates. Single-bit revolving door is easy to be implemented in the experiment, so the realization of quantum controlled not door caught great attention by the people. It has great breakthrough in theory and experiments, for instance, J.I. Cirac and P. Zoller in 1995 proposed ion trap program [9], in 1997 Steane also described these theories in detail [10].

4. Quantum Algorithm

A quantum computer is a computer that obeys the laws of quantum mechanics, and it can support new types of algorithms, quantum algorithms. There are three quantum algorithms that are superior to the classical algorithms: 1. The Fourier transform based on quantum algorithm. Deutsch-Jozsa algorithm, Shor algorithm and discrete logarithm algorithm all belong to this kind of algorithm. Compared with the classical algorithm, this kind of algorithm can accelerate in exponential form. 2. Quantum search algorithm. The basic principle of the quantum search algorithm was found by Grover. This type of algorithm only provides quadratic form of acceleration. 3. Quantum simulation, with quantum computer simulation of quantum systems. The classical computer cannot complete the quantum mechanics system that simulates the natural occurrence.

Here we mainly introduce several major algorithms: quantum Fourier transform, Deutsch-Jozsa algorithm, Shor quantum algorithm and quantum phase estimation.

4.1 Quantum Fourier Transform (QFT)

The quantum Fourier transform is a transformation that exactly corresponds to the mathematical Fourier transform. Quantum Fourier transform is an effective algorithm for Fourier transform of probability range in quantum mechanics [11]. Quantum Fourier transform itself does not accelerate the classical task of Fourier transform of classical data, but it is a key part of quantum factor decomposition and many other quantum algorithms. Discrete Quantum Fourier Transform (DQFT) is a kind of transform that we use more often, which can be considered as a unitary transformation. The effect on the ground state is (choose $|0\rangle, |1\rangle, \dots, |M-1\rangle$ as a set of orthogonal basis)

$$|j\rangle \xrightarrow{DQFT} \frac{1}{\sqrt{M}} \sum_{t=0}^{M-1} e^{2\pi i j t / M} |t\rangle$$

4.2 Deutsch-Jozsa Algorithm

The Deutsch-Jozsa algorithm is an example of a general quantum algorithm [12]. The Deutsch-Jozsa

algorithm is mainly used to distinguish whether the function $f(x)$ is a balanced function or a constant. For all input values, the value of function $f(x)$ may only be 0 or 1. If the function $f(x)$ is an equilibrium function, half of the value of the function $f(x)$ will be 0 for all input values and the other half will be 1. If the function $f(x)$ is constant, the value of the function $f(x)$ is either 0 or 1 for all input values. In the classical algorithm, for the $2n$ input value, to determine whether the exact function $f(x)$ is a balance function or a constant, at least $2n-1+1$ times of tests are required to get a conclusion. But the use of quantum Deutsch-Jozsa algorithm only need once.

4.3 Shor's Quantum Algorithm

In the classic calculation, integer factorization is a problem, the current use of RSA open cipher system is based on this. However, the quantum algorithm discovered by Shor can effectively carry out large factor decomposition, which poses a great challenge to RSA public key system. The quantum algorithm, Shor algorithm, which decomposes the large number factor can successfully transform the NP class problem in classical computation into P class problem [13].

The large number factor decomposition problem is: N is the large odd number known, $N = pq$, figure out P and q . The main steps of the Shor algorithm are as follows:

(1) Randomly take a positive integer y , $y < N$, and is coprime with N , that is, $\gcd(y, N) = 1$. This can be done by the division algorithm.

(2) Define $f(x) = yx \bmod N$, we can see that $f(x)$ is a periodic function, if the period is r , then:

$$y^x \bmod N = y^{x+r} \bmod N$$

Then, $y^x = 1 \bmod N$

(3) Figure out p and q .

$$(y^{r/2})^2 - 1 = 0 \bmod N$$

$$(y^{r/2} - 1)(y^{r/2} + 1) = 0 \bmod N$$

Using division algorithm to figure out the maximum common divisor of $y^{r/2} + 1$ and N , which is p .

The main calculation in the above steps is the division algorithm, to find the $f(x)$ and the period of $f(x)$. The time complexity of the division algorithm is $O(n^2)$. Calculate the time complexity of $f(x)$ as $O(n^2(\lg n)(\lg \lg n))$. The time complexity of Fourier transform is required for getting period of $f(x)$, the time complexity of Fourier transform is $O(\lg n)$, so the time complexity of Shor quantum algorithm is $O(n^2(\lg n)(\lg \lg n))$.

4.4 Quantum Phase Estimation

Quantum phase estimation is the key to many quantum algorithms, which is mainly dependent on quantum Fourier transform [2]. If a unitary operator U has an eigenvector $|u\rangle$, the corresponding eigenvalue is $e^{2\pi i \phi}$ that the unknown phase ϕ is the amount to be estimated by the phase estimation algorithm. The phase estimation process itself is not a complete quantum algorithm, but a subroutine that needs to be combined with other subroutines to complete the computational task. Thus, when performing phase estimation, a black box is used for a controlled operation U^{2^j} (j is a nonnegative integer). The quantum phase is estimated using two registers. The first register contains t qubits and is in state $|0\rangle^{\otimes t}$. The number of selected quantum bits is related to the probability that the number of bits expected to be accurately estimated and the phase estimate is expected to be successful. The second register contains all the quantum bits needed to store the feature vector $|u\rangle$.

5. Conclusion

Quantum computation is based on the basic theory of quantum physics and mathematics, which requires interaction between two-state quantum systems representing quantum bits and can be used for computation. But also through a special external role, to operate and control their state changes in order to achieve the required calculation process from the outside. Quantum computer is a direct application of quantum mechanics in the field of information. Quantum computer research is a very active subject in the field of information science. Compared with classic computer, the algorithm quantum computers use is the quantum algorithm. Based on the nature of quantum mechanics, this paper introduces the background of quantum information science and the status quo of research at home and abroad, and then introduces several quantum algorithms in detail, including Quantum Fourier transform, Deutsch-Jozsa algorithm, Shor's quantum algorithm, quantum phase estimation and so on. We believe that in the future, quantum computer will affect people's life with a large extent, and will improve the conditions of scientific research and speed up the process of scientific progress.

Reference

- [1] YD Zhang. Principles of quantum information physics [M]. Beijing: Science Press, 2008.
- [2] MA Nielsen, IL Chuang. Quantum computation and quantum information [M]. Cambridge: Cambridge University Press, 2000.
- [3] AM Steane. Simple quantum error-correcting codes [J]. Physical Review A, 1996, 54: 4741.
- [4] GL Long, FG Deng, JY Zeng. Recent progress in quantum mechanics fifth volume [M]. Tsinghua University Press, 2011.
- [5] XL Ka. Advanced quantum mechanics [M]. Beijing: Higher Education Press, 2001.
- [6] V. Bužek, SL Braunstein, M Hillery, D. Bruß. Quantum copying: A network [J]. Physical Review A, 1997, 56 (5): 3446-3452.
- [7] A Barenco, CH Bennett, R Cleve et al. Elementary gates for quantum computation [J]. Physical Review A Atomic Molecular & Optical Physics, 1995, 52 (5): 3457.
- [8] A Barenco, D Deutsch, A Ekert, R Jozsa. Conditional quantum dynamics and logic gates [J]. Physical Review Letters, 1995, 74 (20): 4083.
- [9] JI Cirac, P Zoller. Quantum computations with cold trapped ions [J]. Physical Review Letters, 1995, 74 (20): 4091-4094.
- [10] A Steane. The ion trap quantum information processor [J]. Applied Physics B, 1997, 64 (6): 623-643.
- [11] A Ekert, R Jozsa. Quantum computation and Shor's factoring algorithm [J]. Reviews of Modern Physics, 1996, 68 (3): 733-753.
- [12] P Dong. Preparation and application of multi-particle entangled state [D]. Master's Degree Thesis of Anhui University, 2005.
- [13] PW Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. Siam Review, 2006, 26 (5): 1484-1509.