

Analysis of quantum gates in quantum circuits

Rongyuan Cui^{1,†}, Zhuyang Lyu^{2,3,†}

¹Tsinglan School, Dongguan, 523820, China

²Qianweichang College, Shanghai University, Shanghai, China

³275109212com@shu.edu.cn

[†]These authors contributed equally.

Abstract. Although classical computing has brought great convenience to mankind's lives, classical computing is facing some problems. Combining computer science, information theory, and quantum mechanics, quantum information has been developed in many fields. Quantum gates can operate quantum bits, the carrier of quantum information, while quantum circuits are composed of quantum gates and quantum bits, showing the logic of operations. This study summarizes the fundamental concepts of quantum informatics: qubits, quantum circuits, and quantum gates where it is proved that single-bit quantum gates and CNOT gates are universal quantum gates. In addition, this research also demonstrates the current progress of quantum gates in the examination of fidelity of quantum gates, improvement of fidelity of quantum gates, and teleportation of quantum gates. Meanwhile, according to the current development status, the limits and prospects of quantum information are discussed. These results shed light on helping readers understand the basic concepts of quantum information, thus understand the future applications and developments in quantum information.

Keywords: Quantum Bits, Quantum Circuits, Quantum Gates, Universal Quantum Gates, Teleportation Of Quantum Gates.

1. Introduction

Although classical computers increase their ability to computation followed by Moore's Law, they seem to reach their limitation contemporarily, i.e., hard to improve hugely as before. With the minification of their sizes, it is impossible to take the quantum effect out of consideration. Besides, to avoid the weakness of classic computers, scholars also propose some other ways such as crystal valves and quantum dots, where quantum mechanics still dominate [1]. Since the discovery of the concept of quantum, the subject has changed the cognition of the world and sped the creation of a large number of new technologies. Therefore, someone came up with the idea that connects quantum mechanics and computations to break through the limitation. In other words, researchers want to create a computer that is based on quantum logic initially to process information [1].

There are some differences between classical computation and quantum computation. According to Shannon's information theory, the bit, the carrier of information, is widely used in the production and process of information with a binary algorithm. Similarly, the concept of a combination of quantum and bit—qubit—is coined to represent messages in quantum computation. A qubit is a unit vector in the vector space C^2 , which is the superposition of $|0\rangle$ and $|1\rangle$ corresponding to bit 0 and bit 1, respectively.

Besides, the transformations on qubits are unitary, different from the operations in classic. Moreover, the key to quantum information is quantum entanglement. Object to quantum mechanics, Einstein, Podolsky, and Rosen proposed a paradox, which accidentally introduced entanglement into physics [2], blooming quantum information.

Based on the former physical knowledge, Feynman et al. proposed the idea, which is considered as the beginning of quantum computers [3]. Feynman suggested a machine simulating physics directly and then give some basic thoughts about simulating time and simulating probabilities [4]. Afterward, from the reversible system, he gave some reasons that quantum computers can reduce the occurrence of entropy and irreversible interaction and the reduction of their size has no limit [5]. With many years of development, quantum information has achieved greatly in quantum computers, quantum communication, quantum cryptology, and quantum algorithm.

Quantum circuits and quantum gates play an essential role in quantum information. Quantum circuits are channels to transmit qubits and connect different quantum gates, showing the logic of the process, while quantum gates serve as the operation or transformation of qubits. Recently, quantum gates and circuits have gained ample accomplishments. Examination of the fidelity of quantum gates and improvement of fidelity of quantum gates can monitor and advance the accuracy of a quantum process [6-9]. Besides, the teleportation of quantum gates is another way to transmit messages prevalent for modularity and fewer errors [10]. This paper provides a brief introduction to the advantages of quantum bits, quantum circuits, and quantum gates and their future development, as well as pointing out the more cutting-edge scientific discoveries of today and linking them to possible future directions in the discipline. Besides, we also introduce the limitation and prospects of quantum information to urge further study.

2. Quantum Information

2.1. Quantum Bit

It is well known that in classical information theory, we use the bit to represent the carriers by which information is transmitted. A bit is a binary variable whose value is often written as 0 and 1. Therefore, in a classical computer, one can represent all information as 0 and 1 utilizing a binary algorithm, e.g., for an integer N we can represent it as

$$N = \sum_{k=0}^{n-1} a_k 2^k \quad (1)$$

The advantage of using binary for classical bits is that such data is ideally suited for storage in electronic devices [1]. An electronic circuit consists of two parts, wires, and gates, where the bits carry information in the wires and the bits are logically manipulated at the gates, a process that is the input and output of classical information [1]. In analogy to the carrier bit in classical information theory, for quantum information theory, this study will refer to the carrier of information as the quantum bit (qubit). As mentioned before, classical bits have only two states, either 0 or 1, whereas in quantum computing we use Dirac notation and represent quantum bits in a two-dimensional Hilbert space

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2)$$

The classical 0 corresponds to $|0\rangle$, and the state 1 in the classical corresponds to $|1\rangle$ (here the requirement is that it should be orthogonal $|0\rangle, |1\rangle$, i.e., mutually independent). There seems to be little difference between classical and quantum, but according to one of the fundamental assumptions of quantum mechanics: the principle of superposition of states, in quantum information the real state presented is in fact in the form of superposition of states (when not measured) $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers whose squares denote the probability of occurrence rate, respectively, and

to satisfy normalization, there should be $\alpha^2 + \beta^2 = 1$. In contrast, for the case with two quantum bits, four ground states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are obtained by linear superposition [11]:

$$|\psi\rangle = C_{00}(|0\rangle \otimes |0\rangle) + C_{01}(|0\rangle \otimes |1\rangle) + C_{10}(|1\rangle \otimes |0\rangle) + C_{11}(|1\rangle \otimes |1\rangle) \quad (3)$$

By analogy, for n quantum bits, we need a superposition of 2^n basis vectors to get the state of the system. In contrast to classical bits, although the state of a quantum bit is not 0 or 1, in a mixed state, when we measure it, the mixed state eventually collapses to one of $|0\rangle$ or $|1\rangle$ and gives the classical value of 0 or 1 [12], but the quantum computer still has advantages in information storage and information processing that the classical computer does not have. For example, when we study a system of 40 spin one-half particles, a classical computer has to store 2^{40} bits of memory, but a quantum computer only needs 40 quantum bits to solve this problem [13]; when we process the above information, we need to operate 2^{40} several times to ensure that each state is acted upon, but a quantum computer only needs 40 operations. In addition, the entangled state of the quantum can bring many advantages to quantum computing [14].

For a more convenient and visual understanding of quantum bits, we generally rewrite equation (3) in the following form as

$$|\psi(\theta, \phi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \quad (4)$$

This $|\psi(\theta, \phi)\rangle$ can then be considered as a vector pointing from the center of the ball to any point on the ball, and the operations performed on the quantum bits can be considered as rotations of this vector. This ball is then called a Bloch ball [1]. While the above is a mathematical analysis of the concept of a quantum bit, the next step is to describe the quantum bit from a physical point of view. A quantum bit is a two-energy quantum system, and in equation (3) we use $|0\rangle, |1\rangle$, this set of basis vectors, which physically means that a quantum bit is represented by vertically polarized light and horizontally polarized light, as a two-energy system. For example, if one chooses the spin of an electron as the carrier of a quantum bit, it can be considered as the different spin directions of the electron. If we use the energy level state of the electron as the carrier, we can put the two basis vectors corresponding to the case where the energy level of the electron is in the ground state and the excited state respectively [12, 13].

2.2. Quantum Lines

A quantum line, also known as a quantum circuit, can be thought of as a combination of quantum logic gates and quantum bits, in which the effects of each quantum logic gate are understood to be applied in turn to the quantum bits (as shown in Fig. 1). The results of measuring the quantum line are measured using the principle of projection measurements.

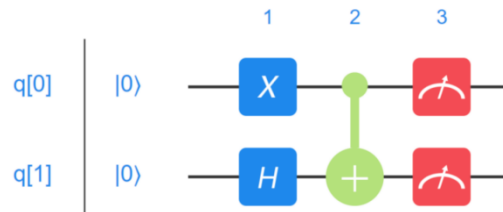


Figure 1. A quantum line with two quantum bits.

The superposition principle can be demonstrated in quantum computing, which relies on the superposition of quantum states, i.e., the coexistence of some quantum states at one time, which is known as "Schrödinger's cat", and the superposition of quanta can be demonstrated by Young's double slit interference experiments on electrons [15] and Wheeler delayed selection experiments [16, 17]. Thereafter, it follows that the state of a computer of size n quantum bits can be expressed as $|\Psi\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle$. Thus, in this quantum circuit, a computer is used as a quantum store to simulate both the

vector of quanta and to store all possible states of quanta at the same time. The advantage of quantum computing is that the superposition of quantum states can be used to vectorize all the results of a quantum without requiring the researchers to input the results multiple times, and the results increase as the number of 2^n quantum bits increases.

2.3. Quantum Gate

In contrast to traditional logic gates and gates and or gates, quantum computers use quanta to perform calculations that can exist in a superposition of "0" and "1" states, which are also dependent on the superposition of quanta and quantum gates are reversible. These quantum calculations rely on quantum logic gates, which are divided into two categories, single-quantum gates, indicated and multi-quantum gates. Single quantum gates are useful because they can switch the state of a quantum bit between "0" and "1", and can be written when the computational base is "0" and "1". "1" can be written in the as $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. The difference between a multi-quantum bit gate and a single quantum bit gate is that it connects two or more quantum bits to perform the algorithm.

In this section, it is shown that single quantum bit gates and double quantum bit controlled non-gates are universal gates for quantum computing, i.e., all quantum gates can be represented by these two quantum gates. Let's first show that the controlled U-gate can be disentangled into a single quantum bit gate and a controlled non-gate. For a controlled U-gate consisting of an arbitrary Missy-positive transformation U acting on a single quantum bit, it means that the quantum gate U acts on the target bit when the control bit is; if the control bit is, then no operation is performed on the target bit. Since any positive matrix requires the rows and columns of the matrix to be orthogonally normalized, we can assume that the correct transformation U is written in the following form.

$$U = \begin{bmatrix} \frac{e^{i(\delta-\frac{\alpha-\beta}{2})} \cos \theta}{2} & -\frac{e^{i(\delta-\frac{\alpha+\beta}{2})} \sin \theta}{2} \\ \frac{e^{i(\delta+\frac{\alpha-\beta}{2})} \sin \theta}{2} & \frac{e^{i(\delta+\frac{\alpha+\beta}{2})} \cos \theta}{2} \end{bmatrix} = \Phi(\delta)R_z(\alpha)R_y(\theta)R_z(\beta) \quad (5)$$

where

$$\Phi(\delta) = \begin{bmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{bmatrix} \quad (6)$$

and R_y, R_z are the matrices that rotate about z and y axes. It can be obtained that for any such matrix U, there are matrices A, B and C

$$A = R_z(\alpha)R_y\left(\frac{\theta}{2}\right), \quad B = R_y\left(-\frac{\theta}{2}\right)R_z\left(-\frac{\alpha+\beta}{2}\right), \quad C = R_z\left(\frac{\beta+\alpha}{2}\right) \quad (7)$$

Hence, $ABC = I$, $\Phi(\delta)A\sigma_x B\sigma_x C = U$. Therefore, one can use the route shown in the Fig. 2 instead of the controlled U-gate. It indicates that when the control bits are $|0\rangle$, the target bits remain the same as the initial state after passing through the quantum gate CBA, respectively. When the control bits are $|1\rangle$, target bits pass through the quantum gate respectively $C\sigma_x B\sigma_x A$, Re-use of logic gates $\Phi(\delta)$ to eliminate the extra phase, we get the same result as if the initial quantum state had been transformed by U.

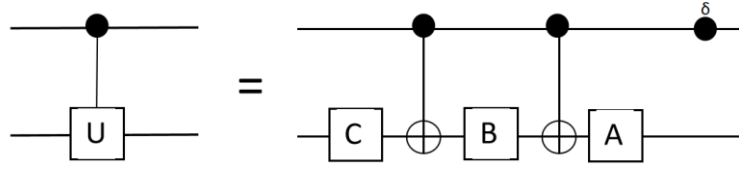


Figure 2. Unitary U can be composed of single quantum gates and 2-bit XOR gates.

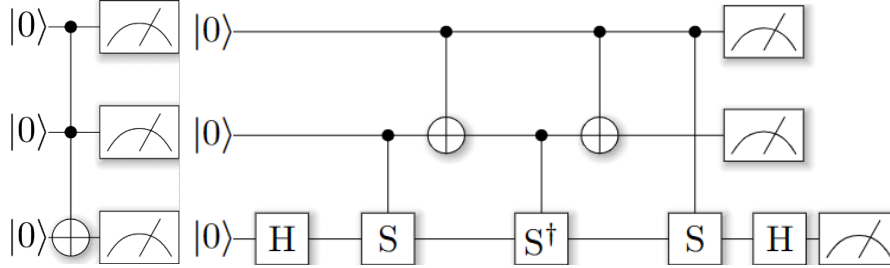


Figure 3. Toffoli gates can be composed of controlled non-gates, controlled U -gates, and Hadamard gates. The left is a Toffoli gate and the right is the alternative circuit, both drawn by ProjectQ.

Quantum Gate $C^k - U$ denotes when the quantum states of all the control bits in the controlled line are $|1\rangle$, Only then is the change U operation performed on the target bit; only the presence of a quantum state of the control bit as $|0\rangle$, then no operation is performed on the target bit. In classical computing, $C^2 - U$ Gates, also known as Toffoli gates, are universal gates and as such have a very important role in classical computing. Likewise, it has a pivotal role in quantum computing. It can be shown that Toffoli gates can be composed of controlled non-gates, controlled U -gates, and Hadamard gates, as shown in Fig. 3. Here, S denotes

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad (8)$$

S and S^\dagger both can be constructed with controlled non-gated single quantum bit gates Having obtained Toffoli's generic quantum gate construction method, it is possible to further generalize it with the help of Toffoli gates and auxiliary quantum bits to obtain any $C^k - U$ gate both can be obtained using single-bit quantum gates and controlled non-gate constructions. For any unitary transformation acting on n qubits, we first use the decomposition formula proposed by Barenco et al. in 1995

$$U^{(n)} = \prod_{i=1}^{n-1} \prod_{j=0}^{i-1} V_{ij} \quad (9)$$

the V_{ij} is to rotate $|i\rangle, |j\rangle$ following a 2×2 unitary matrix. The construction of V_{ij} can utilize the Gray code. The quantum state $|i\rangle$ is transformed into $|i_f\rangle$ state through a generalized gate, so that the Gray code of state $|i\rangle$ is only one digit different from code of state $|j\rangle$. Then, $C^k - U$ gate is used to rotate $|i_f\rangle$ state and $|j\rangle$ state and reversible transformations are operated for used states to restore them. Based on the above process, quantum gate V_{ij} only acting on $|i\rangle$ and $|j\rangle$ is constructed [1, 18]. To put it in a nutshell, it is proved that single quantum bit gates and the CNOT gate are universal logic gates for quantum computing.

3. Applications of Quantum Gate

3.1. Examination of Fidelity of Quantum Gates

It is demonstrated that the information can be coded to the properties of particles, e.g., orbital angular momentum, path, and polarization. Subsequently, it is transmitted and measured along the quantum circuit where quantum gates lie and make operations to the carriers. Based on the process, quantum states and quantum gates are valuable resources for the spread of information. Before using the operations and carriers to compute or transmit, it is essential to examine whether they are satisfied our expectations [7]. Fidelity, a central concept to quantum information, provides a mathematical prescription for the quantification of the degree of similarity of a pair of quantum states, as well as for the examination of quantum gates between the theoretical gates and expected gates [6]. Nowadays, the examination has included: quantum state tomography, direct fidelity estimation, and efficient verification of quantum gates etc. [7].

3.2. Improvement of Fidelity of Quantum Gates

High-quality two-qubit gates with high fidelity are crucial for quantum information processing [8]. Currently, the decrease in the fidelity of quantum gates mainly comes from the following three reasons: imperfect control, non-ideal interactions, and decoherence which is the dominant source in the protocols [19]. For decades, many researchers have struggled for methods to hold high-fidelity gates. One of them is to introduce the idea of adiabatic into quantum gate operations due to the insensitivity of adiabatic characteristics. It is reported that a two-qubit-super adiabatic (TQSA) gate protocol based on parametric modulation enables a fidelity of 94.2% and even higher with higher coherence [7, 8]. Besides, there is a way that combines the conventional time-optimal quantum control strategy with dynamically corrected gates techniques constructing a unitary transformation which is coherence free. This protocol has been proven effective in theory and experiments [9].

3.3. Teleportation of Quantum Gates

With the rapid development of quantum computation, nowadays scientists have come up with a more effective and efficient method to deal with the noise and errors from the environment, i.e., modularity. The modular architecture is a distributed network of modules composed of small components and communicated by both the classical and quantum channels. A small component mainly consists of two parts: data qubit(s) that store and process information and communication qubit(s) that mediate the interaction between different modules. Adopting these circuits, one can isolate the process in the module and there will be less interaction between the different modules, which means the system will keep high efficiency even the scale expands. Initially, scholars realized the state teleportation of unknown quantum states between two modules. Expanding the technique, scientists conceive the teleportation of quantum gates similarly. The chosen gates can implement a unitary operation between two unknown states with a protocol without any direct interaction between the two data qubits. The process of teleportation of CNOT gate can be shown in Fig. 4. D1 and D2 represent data qubits while C1 and C2 represent data communication qubits. The procedures are: (1) C1 and C2 are entangled by the quantum channel, (2) the CNOT gates entangle C1 and D1, C2 and D2 respectively, (3) measure C1 and C2, (4) give feedback to D1 and D2 after measurement [20]. It is demonstrated that the CNOT gate and the controlled-G gate are possible theoretically [10, 20].

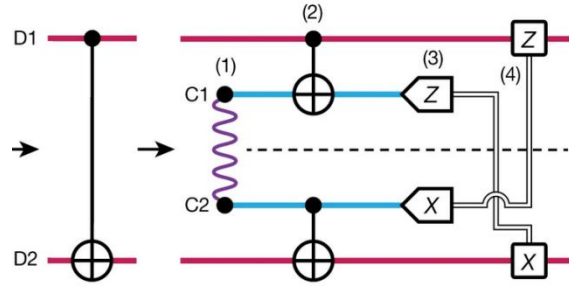


Figure 4. the brief process of teleportation of CNOT gate.

4. Limitations & Prospects

Although quantum information has achieved a multiplicity of accomplishments, it still faces some problems and limitations in quantum algorithms and quantum control systems, which simply means no operable application has been realized. From the software of computation, it is known that the computer needs algorithms to function on the import data then it can output results in classic computers. Similarly, in quantum computers, people also need some algorithms specialized for quantum systems to do calculations or other operations. Algorithms including Shor algorithms, Grover algorithms, and variational quantum eigen solver algorithms have been proposed, but it requires more algorithms applied to quantum computers to realize practical quantum computation. Besides, quantum control systems are also required to improve, where the systems connect quantum algorithms and quantum physics systems. The main challenges of quantum control systems are prompt feedbacks to realize feedback control and a close connection between algorithms and physical systems [21]. Presently, many institutions and companies, e.g., Google and IBM have explored superconductivity-based, optical-based, and other methods-based quantum control systems.

From a short-term perspective, quantum computing can be implemented in quantum simulation, quantum optimization, and quantum-enhanced artificial intelligence. To be specific, compared with the function of approximation of nature in classical computers, quantum simulation is the most fundamental application to simulate the physical principles of nature radically and chemical processes precisely. The accuracy of modeling can be improved, and the efficiency of research and development in areas such as biopharmaceuticals and chemical materials can be enhanced. Hence, in the biomedical field, the middle and latter stages of drug manufacture require a large amount of data modeling and calculation, where very high computing power to analyze the molecular properties of the drug simulation is necessary. On this basis, quantum computers just have an advantage over classical computers. Therefore, quantum computing is a disruptive technological development with enormous potential value in both information science and the future strategic deployment of the resources that underpin quantum information science, which has been developed by leaps and bounds in recent years on all fronts.

5. Conclusion

In summary, we focus on quantum bits, quantum circuits, quantum gates, and their applications. The model of quantum computing has its origins in the Turing computer and is based on the theory of quantum mechanics, which has been verified by numerous experiments since the beginning of the 20th century. It differs from conventional computers in the way it uses storage in the form of quantum superposition states and computation through the evolution of quantum states, thus achieving a quantum computer that takes less time than a classical computer to solve certain computational problems. Due to the current limitations on the number of quantum bits available with current technology, the computation of medium-scale quantum gates may be difficult to achieve applications shortly. Although quantum computers have very many advantages, they can only perform quantum computations that do not require a large number of operations. In the future, quantum computing will have greater development in quantum algorithms, quantum simulation, and quantum system control, to realize the true application of quantum informatics. Overall, these results offer a guideline to learn the basic concepts about quantum

information such as qubits, quantum circuits, and quantum gates. Besides, it is also beneficial for researchers to know the cutting-edge developments, promoting further knowledge of quantum information.

References

- [1] Benenti G 2011 Principles of Quantum Computation and Information Science Press.
- [2] Wang X and Pan J 2022 2022 Nobel Prize in Physics: Quantum Entanglement Science Foundation in China 36(06) pp. 928-930.
- [3] Qin J 2019 Research on Quantum Teleportation and its Route Optimization Hubei University of Technology.
- [4] Feynman R P 1982 Simulating physics with computers Int J Theor Phys 21 pp. 467–488.
- [5] Feynman R P 1986 Quantum mechanical computers Found Phys 16 pp. 507–531.
- [6] Liang Y C, Yeh Y H, Mendonca P E M F et al 2019 Quantum fidelity measures for mixed states. Reports on Progress in Physics.
- [7] Xu Y, Chu J, Yuan J et al. 2020 High-Fidelity, High-Scalability Two-Qubit Gate Scheme for Superconducting Qubits Physical Review Letters 125(24) 240503.
- [8] Zhang R 2022 Experiment Research on Efficient Quantum State and the Quantum Gate Certification University of science and technology of China.
- [9] Ling H 2016 The Time Optimization of Dynamically Error-corrected Quantum Gates and Experimental Verification. East China Normal University.
- [10] Zhang X 2019 Research of Quantum Gate Teleportation and its Fidelity. Zhejiang University.
- [11] Nakahara M 2008 Quantum Computing: From Linear Algebra to Physical Realizations CRC Press.
- [12] Chen H 2006 A Brief Introduction of Quantum Information and Quantum Computin Nanjing: Southeast University Press.
- [13] Zhang Y and Guo G 2000 Quantum computer Science 52(6) pp. 6-9.
- [14] Wu N, Song F, and Li X 2016 Universal Quantum computer: Theory, composition and implementation Chinese Journal of Computers 39(12) pp. 2429-2445.
- [15] Davisson C and Germer L H 1927 Diffraction of Electrons by a Crystal of Nickel. Phys. Rev., 30(6) pp. 705-740.
- [16] Wheeler J A 1978 The “Past” and the “Delayed-Choice” Double-Slit Experiment. MARLOW A R. Mathematical Foundations of Quantum Theory. Academic Press, 1978, pp. 9-48.
- [17] Yin J, Cao Y, Li Y H, et al 2017 Satellite-based entanglement distribution over 1200 kilometers Science 356(6343) pp. 1140-1144.
- [18] Barenco A, Bennett C H, Cleve R et al 1995 Elementary gates for quantum computation Physical Review A 52(5) pp. 3457-3467.
- [19] Chu J 2020 Adiabatic Two-Qubit Gates in Superconducting Circuits Nanjing University.
- [20] Chou K S, Blumoff J Z, Wang C S et al 2018 Deterministic teleportation of a quantum gate between two logical qubits Nature 561(7723) pp. 368-373.
- [21] Li X, Fu X, Yan F, et al. 2022 Current status and future development of quantum computation Engineering Science 24(4) pp. 133-144.