Chapter

Introductory Chapter: Quantum Computing and Communications

Yongli Zhao, Yazi Wang and Xiaosong Yu

1. Introduction

1.1 The origin of quantum information

Quantum mechanics' establishment and development triggered the first wave of quantum technology in the twentieth century. With the regulation and observation of microphysical quantity as the main feature of understanding and grasping the microphysical phenomena and laws, quantum information based on the principles of quantum mechanics was born. Quantum information, a new information method, that calculates, encodes, and transmits the physical information contained in the "state" of a quantum system. The most common unit of quantum information is the qubit, that is, intrinsically linked to each other and can be any combination of 0 and 1 simultaneously.

2. The development history of quantum information

Quantum information technologies aim to use the natural characteristic of the atomic scale to accomplish tasks that cannot be achieved with existing technologies and use the characteristic of measuring or observing a quantum system to change the quantum information fundamentally. These technologies rely on qubits. Meanwhile, scientists are creating physical qubits from a variety of particles, such as atoms or light particles, or objects that mimic them, such as superconducting circuits. Scientists manipulate the quantum properties of each qubit and entangle multiple qubits with each other to create quantum technology from these qubits. These functions support two potential transformative applications, that is, quantum computing and quantum communications. However, quantum information is fragile and can be irreversibly lost through interactions with the environment, a process known as decoherence. Quantum error correction techniques have been proposed and proven, but are challenging to implement. Based on these, researchers began to explore the application of quantum information to quantum technologies in the twentieth century.

- In 1959, researcher Richard Feynman believed that manipulating matter at the atomic scale is possible, meaning that certain types of computation can be done more efficiently on quantum systems than on classical [1].

- In 1972, researchers showed that one qubit measurement could affect other qubits, which is the first proof of entanglement [2].

- In 1981, researchers observed that it might not be possible to effectively simulate the evolution of quantum systems on classical computers and proposed a basic model of quantum computing.

- In 1984, researchers described a quantum key distribution scheme; in this scheme, eavesdroppers had a high probability of being detected when they tried to monitor an encrypted key exchange that used qubits to transmit information. The scheme, often referred to as BB84, is considered the first quantum cryptography protocol [3].

- In 1987, researchers found the property necessary for photon entanglement by measuring the time interval between two photons and found these two photons were indistinguishable from each other [4].

- In 1991, researchers extended the BB84 protocol and introduced a different method of quantum key distribution that contains entanglement [5].

- In 1994, the well-known American physicist Peter Shor proposed the well-known quantum algorithm, which is the Shor quantum decomposition algorithm. The Shor quantum decomposition algorithm is based on the Deutsch-Jozsa algorithm [6], following the laws and theories of quantum mechanics [7].

- In 1998, researchers demonstrated through principle experiments that quantum error correction is possible, which is necessary for cost-effective quantum computing and communication because excessive noise can destroy quantum information.

In the twenty-first century, the theory and development of quantum computing and communications puts this significance on a firm footing and leads to some new profound and exciting insights into the natural world. From 2000 to 2005, a variety of time-efficient quantum algorithms were proposed, such as the semi-product groups [8–10], the near-Hamiltonian groups [11], the normal subgroups [12, 13], the almost Abelian groups [14]. In 2006, Hayashi et al. [15] proposed the first quantum network coding scheme, which realized the cross transmission of two qubits in a full quantum channel butterfly network. Due to the constraints of quantum properties, such as the quantum unclonable theorem, this scheme cannot achieve lossless quantum transmission, that is, the fidelity is less than 1. In 2012, Satoh et al. [16] designed a novel quantum network coding scheme using quantum repeaters. In 2014, Nishimura [17] summarized the current state of quantum network coding, discussing the nature of quantum network coding schemes using entangled resources to communicate with classical. In 2020, Wu et al. [18] proposed a continuous-variable quantum network coding scheme based on a butterfly-shaped network model.

3. Quantum revolution with quantum computing and communication

Among these, some quantum computing and communication technologies are available for use; for example, quantum computer, quantum cryptography, teleportation, and quantum error correction. Quantum computer is the physical platform that realizes quantum computing to encode qubits so that different qubits can be coupled in a controllable manner and have a certain resistance to the influence of the noise environment. The main quantum computer solutions currently developed include superconductivity, ion traps, quantum dots, topologies, and diamond color centers. Quantum cryptography can take advantage of quantum states to enable classical information to be transmitted securely. Teleportation achieves reliable

transmission of quantum states by using entanglement. Quantum error correction keeps the possibility of maintaining quantum coherence when an irreversible noise process exists.

At present, the world is undergoing a new round of "quantum revolution". Quantum computing and communication technologies are accelerating breakthroughs in key technologies. In the new stage, some technologies are gradually being integrated with the system. Breakthroughs have been made in key technologies, such as integration, engineering, and networking. The integration of quantum communication with classical communication networks, multi-bit operation, and computing of quantum computers show the application prospects of quantum information in the industry.

4. Brief introduction of the book

In this book, we will introduce some fundamental quantum computing and communication technologies that will form the basis for much of what follows. After this brief introduction, we will review the basic conception and relevance of quantum algorithms, quantum computer, quantum code, post-quantum cryptography, quantum key distribution, and quantum teleportation respectively in detail.

Author details

Yongli Zhao*, Yazi Wang and Xiaosong Yu
Beijing University of Posts and Telecommunications, Beijing, China

*Address all correspondence to: yonglizhao@bupt.edu.cn

References

[1] Feynman R. There is plenty of room at the bottom: An invitation to enter a new field of physics. In: Lecture at American Physical Society Meeting. Vol. 29. 1959

[2] Freedman SJ, Clauser JF. Experimental test of local hidden-variable theories. Physical Review Letters. 1972;**28**(14):938-941

[3] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: International Conference on Computers, Systems, and Signal Processing. 1984. pp. 175-179

[4] Hong CK, Ou ZY, Mandel L. Measurement of subpicosecond time intervals between two photons by interference. Physical Review Letters. 1987;**59**(18):2044-2046

[5] Eckert AK. Quantum cryptography based on Bell's theorem. Physical Review Letters. 1991;**67**(6):661-663

[6] Deutsch D. Quantum theory, the church–Turing principle and the universal quantum computer. In: Proceedings of the Royal Society of London, A, Mathematical and Physical Sciences. 1985

[7] Shor P. Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science. 1994. pp. 124-134

[8] Kuperberg G. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM Journal on Computing. 2005;**35**(1):170-188

[9] Moore C, Rockmore D, Russell A, et al. The power of basis selection in Fourier sampling: The hidden subgroup problem in affine groups. In: Proc. SODA. 2004

[10] Yoshifumi I, Le Gall F. Efficient quantum algorithms for the hidden subgroup problem over a class of semi-direct product groups. arXiv preprint quant-ph/0412033. 2004

[11] Gavinsky D. Quantum solution to the hidden subgroup problem for poly-near-Hamiltoniangroups. Quantum Information and Computation. 2004;**4**:229-235

[12] Hallgren S, Russell A, Ta-Shma A. Normal subgroup reconstruction and quantum computation using group representations. SIAM Journal on Computing. 2003;**32**(4):916-934

[13] Ivanyos G, Magniez F, Santha M. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. In: SPAA. New York: ACM Press; 2001. pp. 263-270

[14] Grigni M, Schulman L, Vazirani M, et al. Quantum Mechanical Algorithms for the Nonabelian Hidden Subgroup Problem. In: Proceedings of the thirty-third annual ACM symposium on Theory of computing; 2001. pp. 68-74

[15] Hayashi M et al. Quantum network coding. In: Annual Symposium on Theoretical Aspects of Computer Science. Berlin, Heidelberg: Springer; 2007

[16] Satoh T, Le Gall F, Imai H. Quantum network coding for quantum repeaters. Physical Review A. 2012;**86**(3):032331

[17] Nishimura H. Quantum network coding and the current status of its studies. In: 2014 International Symposium on Information Theory and its Applications. IEEE; 2014

[18] Qu Z et al. Continuous-variable quantum network coding protocol based on butterfly network model. International Journal of Sensor Networks. 2020;**32**(2):69-76