ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 168

International Conference on Modeling, Analysis, Simulation Technologies and Applications (MASTA 2019)

Research on Quantum Computing Technology and Application

Meng-liang LI*, Hong YANG and Xiong GUO

China Electronics Standardization Institute, China

*Corresponding author

Keywords: Quantum computing, Concepts, Technology, Applications, Development trend.

Abstract. Quantum computing is a novelty type of calculation mode that follows the rules of quantum mechanics regulating quantum information units. The general theoretical model of a quantum computer is a universal Turing machine that is reinterpreted by using the laws of quantum mechanics. Quantum computing can greatly improve the computational efficiency through the principle of quantum superposition, which is widely used in artificial intelligence (AI), accurate weather forecast, traffic congestion management and other fields. In the past 10 years, quantum computing has been increasing in technology, the number of products and the scale of industry. This paper will introduce the history, concepts, current research status, main technology and applications of quantum computing, and the development trends of quantum computing will be presented.

Introduction

For most of computing history, the foundational hardware technology has been binary digital transistor logic. In such digital systems, data and programs are encoded into binary digits (bits) based on two states: on and off. The field of quantum computing introduces a whole new approach to the underlying computing hardware by shifting from simple binary (two-state) logic to a more powerful multi-state logic using a new notion of bit, known as “quantum bits” or “qubits” which are represented by quantum as superposition and entanglement[1].

This shift from a binary digital representation found in today’s conventional computers to a quantum digital representation in tomorrow’s computers will bring huge increases in computing power and new, innovative software that handles today’s hugely complex distributed computational problems and provides more powerful analysis of today’s complex data patterns [2]. Quantum computing holds the potential to revolutionize fields from chemistry and logistics to finance and physics.

However, the increase in power and capability that quantum computing will provide, will also be seen as a dire threat because it can easily defeat today’s encryption mechanisms, which have all been built using pre-quantum computing approaches. As strong as today’s encryption mechanisms have been, they wouldn’t stand a chance against a quantum computing-based attack. This widely known risk associated with the power of quantum computing is very concerning for governments, institutions and individuals whose encrypted files are safe today, but may not be in 10-20 years when quantum computing takes off [8].

This paper will provide the history of quantum computing and its concepts. it will summarize the current research status, main technology and applications of quantum computing, as well as summarize the development trend associated with quantum computing.

Basic Concepts of Quantum Computing

Definition

Quantum computing is a fresh type of calculation mode that follows the rules of quantum mechanics regulating quantum information units. Quantum computing is a kind of parallel computing, which takes entangled quantum states as the carrier of information transmission, and uses the linear superposition principle of quantum states to complete the parallel computing and ultimately get the required information. Quantum computers have very high parallel computing power, which can be

solved in acceptable time by solving some difficult computing problems, such as massive decomposition and complex path search, which is almost impossible for classical computers. The development of information processing technology based on quantum computing is expected to promote new developments in many fields such as large data and in-depth learning, artificial intelligence, information cryptography, chemical materials and drug synthesis. In the future, quantum technology will provide unprecedented powerful tools for social development, such as science, government, finance and national security[3]. Quantum computing includes Gate-based quantum computer and quantum annealing.

a) **Gate-based Quantum Computer.** Quantum computing can greatly improve the computational efficiency through the principle of quantum superposition, which is widely used in artificial intelligence, accurate weather forecast, traffic congestion management and other fields. However, from the point of computational efficiency, due to the superposition of quantum mechanics, quantum algorithms in some problems are faster than traditional computers in dealing with problems. Quantum computer described above is called as Gate-based Quantum computer.

b) **Quantum Annealing.** Quantum annealing is adiabatic quantum computing which find the global minimum of function by a process using quantum fluctuation. Quantum computer which performs Quantum annealing is called as Quantum annealer. The D-Wave machine is the first product of Quantum annealer.

Value

Quantum computing can help shape the ideas of developers, improve the programming methods of traditional computers. Quantum computing can speed up the solution of your problems, not replace the classical computer. Classical computers can speed up your computational algorithms when applying quantum computing, solving some problems that classical computers can't solve. Another value is the hybrid algorithm, which uses both quantum and classical computing resources, making full use of classical computers to deal with most of work, a small part of the calculation is handed over to quantum hardware. New algorithms of quantum computing will emerge, which will bring a lot of business opportunities to our life. But this situation mainly depends on the development of hardware and the progress of software[4]. The convergence of algorithm efficiency is beyond our estimation. Quantum computing uses the principle of quantum mechanics to transmit and process information. It has the advantages of high security and high capacity. Nowadays, the situation of network information security is becoming more and more complex. Quantum computing has become the focus of attention in the global information and communication industry. Among them, quantum teleportation technology, which can directly transmit information, is still in the exploratory stage of experimental research and is the frontier hot spot of basic scientific research in the field of quantum information. Quantum secret communication technology with quantum key distribution as the core can greatly improve the security of information transmission of existing communication technology. It has broad application prospects in government, finance, diplomacy, military and other fields. In recent years, it has developed rapidly in technology research, pilot application and industrial promotion.

Current Research Status of Quantum Computing

United States. The United States was the first country to list quantum information technology as a national defense and security research and development program. As early as 2002, the Defense Advanced Research Projects Agency (DARPA) of the U.S. has formulated the Quantum Information Science and Technology Program, and revised version 2.0 in 2004, giving the development steps and timetable of Quantum Computing. In 2008, DARPA launched the Semiconductor Quantum Chip Research Program called the Micro Manhattan Project, and even ranked QC research as an equally important level as the development of atomic bombs.

China. China has begun to pay more attention to the research of quantum computing and made some achievements in the layout of scientific research and enterprise investment in recent years.

Research institutes such as Chinese academy of sciences, Zhejiang University and Tsinghua University have made some achievements in the experiment of quantum computing principles and prototype development. China University of Science and Technology and Zhejiang University jointly announced that 10-bit entanglement manipulation based on superconducting quantum computing scheme was realized. In terms of industrial layout, Alibaba and the Chinese Academy of Sciences set up the "CAS-Alibaba Quantum Company Laboratory" in 2015.

Europe. As the birthplace of quantum theory, Europe attaches great importance to the impact of quantum information technology on national security and economic development, and has invested a lot of resources to develop quantum technology. The European Union said it had provided long-term support for quantum technology for 20 years, with a total investment of 550 million euros[5].

Other Countries. In addition, South Korea, Japan, Singapore and other technological powers have released their own "quantum information science development plan". At present, South Korea, Singapore focus their research on quantum communication, and also conduct quantum computing research.

Main Technology of Quantum Computing

Quantum Hardware

Quantum hardware is the main bottleneck for large-scale commercial applications of quantum. The one target of quantum hardware is to realize the physical system of quantum computing. The technical path of quantum computing includes liquid NMR, quantum optics and solid-state system.

Quantum Coding

The main target of quantum coding is to overcome the decoherence process that destroys the quantum coherence and ensure the reliability of the calculation. The technical path of quantum coding includes quantum error correction code, quantum error-averse code and quantum error-correcting code.

Quantum Algorithm

Quantum algorithm is designed to provide solutions or improve computational efficiencies for problems that are believed hard to solve with a classical computer. The main quantum algorithms includes Shor's algorithm, Grover's algorithm, HHL algorithm and Hamiltonian simulating algorithm[6].

Relevant Standardization Activities of Quantum Computing

ITU-T SG 13 (future network) initiates new WI on QKD network framework, SG17(Security) initiates study on QKDN security and QRNG in 2018. In 2019, SG13 initiates new WIs on QKD network architecture and key management; SG17 initiates 3 new WIs on QKDN security requirements. SG 17 focused on security. Security guidelines for applying quantum-safe algorithms in 5G systems was started in March 2018.

ISO/IEC JTC 1established SG 2 and SC7/SG 1on quantum computing. 2 new work items ISO/IEC 23837-1 and 2 on QKD security, and the Advisory Group (AG) on Quantum Computing established.

Applications of Quantum Computing

Communication Encryption

Nowadays, the security of all kinds of cryptography relies on all kinds of cryptographic algorithms, but for quantum computers, it is easy to crack them in high-speed parallel through specific algorithms. Based on the characteristics of quantum entanglement, in the process of communication, if someone wants to eavesdrop on the content of communication and measure quantum, the quantum at the other end will inevitably be perceived, thus terminating the transmission of confidential information, commercial secrets can be adequately guaranteed.

Data Computing

The core function of quantum computer is naturally data computing, super high computing power, which is necessary for many industries. For example, the direction of artificial intelligence in this year's big fire, through in-depth learning, constantly improve the algorithm until the product meets people's intelligent needs.

Scientific Research

In the field of scientific research, quantum simulation using quantum computing can bring practical help to the frontier scientific research fields such as quantum chemistry, superconducting physics, quantum field theory. It is difficult to simulate the metabolism of ferredoxin in photosynthesis by molecular dynamics on classical computers, but it can be simulated in one hour theoretically on quantum computer. Google has made the first fully scalable quantum simulation of hydrogen molecule with a quantum computer, which can quickly and accurately simulate the quantum state structure and energy of hydrogen molecule. Quantum computing can simplify complex simulation experiments and calculations which will vigorously promote the scientific development of mankind.

Development Trends of Quantum Computing

The Strategic Commanding Point of Information Technology in the Future

QC is an important development direction of computer technology and be the strategic commanding heights of future information technology. The research of QC includes two parts: dedicated quantum computers (quantum simulators) and general quantum computer[7]. Dedicated quantum computers are mainly dedicated hardware for specific algorithms. Because quantum simulation is easy to implement based on the existing technical conditions, it is expected to become the first practical technology in the field of quantum computers. With the rapid development of quantum computing hardware technology, the core technologies such as small and medium-scale quantum bit integration, high-fidelity and high-speed quantum logic gates, and long-term quantum storage and so on have been breaking through.

QC Will Be Widely Used in Encryption and Decoding in the Future

Network security mostly depends on the difficulty of decomposing large numbers into prime numbers. Although existing digital computers can achieve their goal by searching for every possible decomposition factor, the huge amount of time required will make the decoding process expensive. Quantum computers are exponentially more efficient in decomposition factors than digital computers, which means that traditional security methods will soon become the past. Despite the time required, the development of new encryption methods is under way. Quantum encryption using quantum entanglement as one-way property is also worth looking forward to.

Summary

In this paper, we present the history, concepts, current research status, main technology and applications of quantum computing. At last, the proposed development trends of quantum computing will be used in information technology, encryption and decoding in the future. Quantum computing is approaching the stage of commercialization and has great potential to change our world. It is possible to make breakthroughs in building new business models by quantum computing.

Acknowledgement

This research was financially supported by the ISO/IEC JTC 1/SG2 "Quantum computing".

References

[1] M. Nielsen and I. Chuang, 2016, “Quantum Computation and Quantum Information,” Cambridge University Press, p. 189.

[2] P. Kaye, R. Laflamme, and M. Mosca, 2007, An introduction to quantum computing. Oxford University Press.

[3] Roetteler, and K.M. Svore, 2018, "Quantum Computing: Codebreaking and Beyond." IEEE Security & Privacy 16, no. 5: 22-36.

[4] E. Mount, C. Kabytayev, S. Crain, R. Harper, S.-Y. Baek, G. Vrijsen, S.T. Flammia, K.R. Brown, P. Maunz, and J. Kim, 2015, “Error compensation of single-qubit gates in a surface-electrode ion trap using composite pulses,” Physical Review A, 92:060301.

[5] J. Preskill, 2018, “Quantum Computing in the NISQ era and beyond,” preprint arXiv: 1801. 00862.

[6] M. Reiher, N. Wiebe, K.M. Svore, D. Wecker, and M. Troyer, 2017, “Elucidating reaction mechanisms on quantum computers,” Proceedings of the National Academy of the Sciences of the United States of America, 114: 7555-7560.

[7] D.W. Berry, A.M. Childs, A. Ostrander, and G. Wang, 2017, “Quantum algorithm for linear differential equations with exponentially improved dependence on precision.” Communications in Mathematical Physics, vol. 356, no. 3: 1057-1081.

[8] IOS/IEC JTC 1. JTC 1 Technology Trend Report 2018: Quantum Computing.