SOME PROBLEMS ON QUANTUM COMPUTATION

Byung-Soo CHOI

Department of Applied Physics, University of Tokyo, Tokyo 153-8902, JAPAN

bschoi3@gmail.com

ABSTRACT

In this work, we touch several issues on the quantum computing. First, we touch one of the most practical quantum application such as quantum machine learning. Second, we investigate some ways for secure quantum computation and their problems. Lastly, we discuss the resource overhead problems of fault-tolerant quantum computation and some candidate solutions.

FUNDAMENTAL PRIMITIVES OF QUANTUM INFORMATION FROM THE ICT PERSPECTIVE

Quantum information is defined as an information unit based on quantum mechanics. Since quantum mechanics allows to prepare a superposed state, their interference, their collapsing measurement, their spacetime correlation, quantum information is believed to return huge gain on the ICT (Information and Communication Technology) perspective. For example, by combining the properties of collapse of quantum information with measurement and lots of orthogonal measurement basis, we can easily derive the one-time key generation and distribution protocol, which is called quantum key distribution protocol. By combining the linearity of unitary operators, the constructive and destructive interference, and the superposed state, we can implement the quantum level parallel interference engine, which is widely used for quantum amplitude amplification protocol and for quantum Fourier transform. In addition to that, by sharing the predefined entanglement between the computational nodes, we can reduce the necessary communication overhead.

Though it is too early to consider the full spectrum of quantum ICT, several works have already started to use it for real world situation. In this work, we will discuss some practical applications and their practical problems which should be resolved.

QUANTUM MACHINE LEARNING AND ITS PROBLEMS

Machine learning is a kind of classification of data based on a known or unknown structure. Since the most of ICT applications are based on the effective and efficient classical of raw data, machine learning techniques are practically important. Since machine learning requires a good learning model and the demanding computing power, it has been widely believed that the quantum computing can be helpful very much. Related to this, several works have been proposed such as Supervised and Unsupervised machine learning techniques.

One of the most important problem is to manage the classical data on the quantum bigdata system. Since the quantum machine learning can only work on the quantum memory, and the real world data is the classical data, classical information should be changed into quantum information. Meanwhile to exploit the quantum computational power such memory space and their information retrieval system should be very effective.

As a potential solution, we will discuss the potential advantage of using the recently proposed fixed-point Grover search and its relation with the interaction graph structure.

SECURE QUANTUM COMPUTATION AND ITS PROBLEMS

Considering the price of quantum computing and the sensitivity of user information, we believe that the quantum computing service should be done under very high security. Although the quantum key generation and distribution can help to make the classical channel more secure, it is not sufficient to protect the quantum memory and computing system from any internal or external adversaries. Related to this, the quantum Fully Homomorphic Encryption and Blind Computation models have been proposed. Theoretically they can support almost secure or privacy aware quantum computing.

However, such privacy aware computing can be implemented without overhead. Even such overhead seems to be exponential. Therefore, the first motivation of quantum computing might be nullified with the condition of privacy aware computing. Therefore, it is very necessary to make more cost-effective secure or privacy aware model.

As a potential solution, we will discuss how to combine the quantum error-correction and quantum encryption scheme, which is called quantum cryptcoding.

FAULT-TOLERANT QUANTUM COMPUTATION AND ITS PROBLEMS

To utilize the quantum ICT, we should have a large set of protocols and components. Among them, the most important protocol is the fault-tolerant quantum information processing. Since any quantum information device cannot be isolated from the classical and quantum environment, there is some degree of errors. Unfortunately such small error can ruin the whole gain of quantum information because of quantum decoherence is too fast. Therefore, the practically most important is to implement the quantum information device fault-tolerantly. Related to this, we have lots of protocols from the basic way borrowing the classical methods to the quantum genuine approaches. Therefore we already have lots of solutions.

Unfortunately such fault-tolerant protocols cannot work without overhead. Technically such overhead comes from the necessary redundancy for fault-tolerance, and hence it cannot be avoidable. However, since such overhead is too big, the desired performance gain of quantum information cannot sufficiently higher than the best classical approaches. Therefore, any resource reduction methods for fault-tolerance are very important.

As a potential solution, we investigate fault-tolerant QEC conversion schemes, which can be used for resource optimal computation and interface between computer and communication networks.

SUMMARY

Since the current quantum information research is entering the third phase, practical use for ICT platform, the number of real world problems increases rapidly. Hence we hope many more applied mathematics researchers have interests on this quantum ICT research field.