Research plan on quantum computation.

Duc Manh Nguyen *

September 2, 2019

Abstract

In this report, I firstly introduce myself, my research profiles on quantum information processing during my Ph.D time at University of Ulsan, South Korea. In addition, I briefly describe my research trend on next two years. I hope you can give some advises and provide research fund to make my plan be real and have valuable outcomes.

1 Brief profile

My full name is Nguyen Manh Duc (Nguyen is my family name). I was born in Viet-Nam. I received the bachelor degree in electronic and telecommunication engineering from Ha-Noi university of science and technology (HUST) in 2012. From 2012 to 2014, I was a software engineer at Samsung Electronic VietNam (SVMC). From 2014 to 2015, I was a system engineer at Advance Network System VietNam (ANSV), VNPT group. From 2015 to present, I have been studying for the Ph.D. degree in school of Electrical Engineering, University of Ulsan, Korea.

At University of Ulsan, my research topic includes some hot topic on quantum error correction codes, quantum algorithms, quantum walks. Then, I have published 9 international journals, and around 4 international conferences (the detail is attached in my CV, and I briefly explain them later). In addition, I also was invited as reviewer for some international journals such as IEEE Access, INJP; and was the technical committee of some international conferences such as INFOCOMP 2019, ICTCC 2019.

2 Background

Quantum computation is one of the most important applications of quantum mechanics and give us effective solutions for difficult problems, such as factoring large integer numbers in polynomial time (Shor algorithm), searching in un-ordered sets (Grover search), and increasing the security of quantum cryptography (no-cloning algorithm, measurement destroys the quantum state, and

*It is my personal report. Email: nguyenmanhduc18@gmail.com

entanglement); these tasks are difficult to do using classical computation. However, the effects of noisy and imperfect environments in a quantum channel can affect the performance of quantum computation. Therefore, quantum error correcting codes (QECCs) have been used to achieve fault-tolerant quantum computation. The purpose of my research on quantum error correction codes is to design the channel code (QECC) for quantum channel. Quantum stabilizer code is a kind of QECC constructed based on stabilizer formalism. The most important advantage of stabilizer formalism is that quantum errors that affect an encoded quantum state can be diagnosed and removed by a group of quantum operators, thereby stabilizing this encoded quantum state. In addition, the stabilizer formalism allows quantum codes to be presented by classical error correction codes. Therefore, quantum stabilizer codes can be constructed from binary error correction codes if they satisfy a symplectic inner product (SIP).

In my research, I focus on the construction of quantum stabilizer codes since its advantages on relationship between classical codes and QECC. My consideration construction are:

- I propose the construction of quantum stabilizer code from a suitable difference set (DS). From the suitable DS, the circulant matrices are designed and used to construct the parity-check matrix. Then, the generators of the stabilizer should first be chosen to make independent rows of parity-check matrix. Finally, the codeword and minimum distance are determined. Two quantum stabilizer codes with lengths of seven and 15 from the proposed design are shown to express the practical application.

- To propose a new approach to the construction of additive codes over GF(4), which are self-orthogonal with respect to Hermitian product. The minimum distance of this classical linear code was proved to be 4 in all cases. The corresponding quantum stabilizer code can be transformed from this classical code; we prove all the optimal codes that can be accomplished from this construction with lengths 5, 6, 7, 8, 9, and 10.

- To propose the new construction of quantum codes from symmetric matrices that are based on the CSS structure. The parity-check matrices are first generated from two constructions and proven to satisfy the symplectic inner product for the construction of binary and non-binary quantum stabilizer codes. Then, the parameters of these codes are calculated and explained in detail. Some quantum codes are proven to achieve equality of the quantum singleton bound.

- To propose a new construction of self-orthogonal trace-inner product codes over *GF(4)*. From two binary vectors, we generate the circulant and modified circulant matrices, and the generator matrix for Quaternary linear codes is proposed. Then, the quantum stabilizer codes are derived from the linear codes. The advantage of the proposed construction is that our proposed codes give various dimensions of QECCs, and these minimum distances have good values.

- To propose novel approaches to construction of entanglement-assisted quantum error correction codes. First, we propose a new method for the construction of the isotropic subgroup based on circulant matrices. Then, the entanglement subgroup can be determined from a method of transforming the isotropic group into standard form; hence, the parameters of codes are found, and for effective preparation of the entangled state, the number of ebits should be as few as possible. To explain the practical construction of the quantum codes, design of the proposed EAQECC with lengths up to 12 are shown. In addition, the minimum distance is calculated and explained to show that the proposed construction has good correctable capability, in comparison with recent EAQECC.

In addition, I also have been researching on some others specific fields of quantum computation such as quantum algorithms, quantum walk, and quantum three-stage protocol. The details of my researches are as follows.

- In quantum algorithms, I focused on the outstanding algorithms. Originally, the purpose of the Deutsch-Jozsa (DJ) algorithm is to determine the type of function f that had been used (balanced or constant) via quantum system by using only one query. The main aim of this paper is to propose a modified generalization of the Deutsch-Jozsa algorithm in a d-level (qudits) system to determine the type of function f (constant or linear) used. The proposed algorithm also required only one query in comparison with the classical case. In addition, the quantum key distribution protocol based on the algorithm is discussed to show the contributions of our work to improving the detection of Eve's attack, which cannot be distinguished by the protocol based on the original Deutsch-Jozsa algorithm.

- Quantum three stage protocol (QTSP) is a new kind of quantum cryptography protocol based on Shamir's three-stage protocol of classic cryptography. QTSP shows that there can be no key shared between the sender and receiver unlike the BB84 protocol. The basic idea behind QTSP is that of sending secrets (or valuables) through an unreliable courier by having both Alice and Bob place their locks on the box containing the secret, which is also called double-lock cryptography. I propose a modified QTSP to attach many bits into a single quantum state, and then use the QTSP protocol for the transfer between parties. The proposed protocol promises the advantages of a single qubit that can carry an unlimited amount of information. Moreover, the qubit needs to be protected from noise for the correct quantum state exchanged between parties. Therefore, we use the quantum error correction code emerging with QTSP to restore a quantum noise, the decoherence in a quantum state to a pure quantum state by removing the errors.

- As a quantum analogue of classical random walks and the same motivation as classical random walks, QWs are devised as the mathematical basis to develop sophisticated algorithms. Unlike random walks transformed by

the probability transition matrices on the probability distribution, QWs are transformed by unitary revolutions. The probability distributions of quantum states are defined as the sum of squares of the norms of amplitudes. Due to the quantum interference effects, there exists a non-linearity map between the quantum state and the probability distribution. As a result, QWs have been shown to outperform random walks at certain computational tasks. We propose the further investigation shows that in the one-dimensional quantum walk model, the quantum walks over the one-dimensional infinite line can be based on N-cycles and can not be based on N-lines.

3 Future plan and expected results

Based on my research topics on Ph.D time, in the next two years, I plan to drive my researches focusing on the quantum algorithms, quantum computation, and also quantum machine learning.

(1) From the design of quantum error correction codes from stabilizer formalism, we can get the stabilizer groups. Not only we gain the error correction from these group via syndrome calculation but also we get the full entanglement state, stabilizer frames. The stabilizer group help us on designing of quantum circuit model, quantum key distribution protocol, the design of stabilizer frames which can be used on boosting quantum circuit.

(2) In quantum computation, I will focus the designing of quantum circuits which help to solve some algorithms. Beside it, there are two main quantum basics algorithm that helps us to solve many classical problems. The first one is the quantum phase estimation (QPE) algorithm which help us to determine "qubit state of estimated value" from "inputted ancillary qubits" (the positive real value between 0 and 1 can be estimated into quantum state by quantum circuit of Fourier transform, Hardamard gates, and a special Controlled gate). The second one is Controlled rotation which help us to transfer from the "qubit state of estimated value" to "basis state" with the inversion value of estimated phase.

(3) The study of quantum machine learning focus on designing quantum algorithms that can solve machine learning problems faster than the classical methods. Some main problems of classical ML are as follows.

- Reducing the dimension's of a huge data set. It can be viewed as a compression algorithms or source coding. In quantum, it can be considered by using the principle component analysis (PCA), wavelet transform, fractal compression, or JPEG,... I propose the quantum compressed version based on classical compression and apply it to quantum image for transformation, compression,...

- Quantum neuron network (QNN): Since Grover search algorithm uses the Amplitude amplification, I can view it as a neuron network. The quantum

walk is the general case for Grover search. It promises the QNN can be modified from Grover search and quantum walks.

- The object detection or tracking can be considered to be better by applying quantum computation.
- One application of ML is to estimate quantum state. The quantum state can be estimated and approximated via the data set which include via many measurement. It promises the application of quantum image, video, media, or related.

(4) Currently, there are some open source to implement quantum computation and quantum algorithm such as IBMQX. I plan to research on this setups to test, implement out standing algorithms, and our proposed algorithms.

4 Conclusions

The above information are my research trend for next two years. Based on this plan, I hope to publish around 4-6 SCI/SCIE international journals or can do some project on reality on quantum computer. I hope these can contribute to make quantum computer is better and be reality soon. Thank you so much for reading my plan. I hope you can give some advises based on my plan and we can have great cooperation between.