UNIVERSITI PUTRA MALAYSIA

QUANTUM PROCESSING FRAMEWORK AND HYBRID ALGORITHMS FOR ROUTING PROBLEMS

MOHAMMAD REZA SOLTAN AGHAEI

FSKTM 2010 5

QUANTUM PROCESSING FRAMEWORK AND HYBRID ALGORITHMS FOR ROUTING PROBLEMS

MOHAMMAD REZA SOLTAN AGHAEI

DOCTOR OF PHILOSOPHY
UNIVERSITI PUTRA MALAYSIA

2010

MOHAMMAD REZA SOLTAN AGHAEI Doctor of Philosophy 2010

QUANTUM PROCESSING FRAMEWORK AND HYBRID ALGORITHMS FOR ROUTING PROBLEMS

By

MOHAMMAD REZA SOLTAN AGHAEI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

May 2010

Dedicated to my wife; Zohreh Montazeri

And to my kids; Elaheh and Ehsan

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

QUANTUM PROCESSING FRAMEWORK AND HYBRID ALGORITHMS FOR ROUTING PROBLEMS

By

MOHAMMAD REZA SOLTAN AGHAEI

May 2010

Chairman: **Zuriati Bt Ahmad Zukarnain, PhD**

Faculty: **Computer Science and Information Technology**

The theory of quantum complexity determines when quantum computers may offer a computational speed-up over classical computers. At present, there are only a few general well-known techniques in the field of quantum computing and finding the problems that are amenable to quantum speedups is a high priority. Nonetheless, efficient quantum algorithms are very limited in number and scope; no real breakthrough has yet been achieved in physical implementations. Most importantly, these algorithms are not still matured adequately to be applied in real quantum computations.

The Quantum Processing Unit (QPU) is the processor of quantum computer that is able to do quantum computations. A typical component in QPU is a quantum device that runs quantum algorithms; namely *Quantum Algorithm Processing Unit* (QAPU). The focus of this study is developing a framework of QAPU and hybrid architecture for classical-quantum algorithms. The framework is used to increase the implementation performance of quantum algorithms. The framework shows a general plan for the architecture of quantum processor which is capable to run the quantum algorithms. In particular, QAPU can be used as a quantum node to design a quantum multicomputer.

A uniform platform was proposed for the QAPU used in the present study. At first, the hybrid architecture was designed for the quantum algorithms. Then, the relationship between classical and quantum parts of the hybrid algorithms were extracted and the main stages of the hybrid algorithm were determined. Next, the framework of QAPU was designed and developed. For this purpose, some gates and connections were projected in the framework which could be applied for future quantum algorithms. Furthermore, the framework was set up, implemented and simulated for the existing quantum algorithms on a classic computer. The results were shown that the framework is appropriate for the quantum algorithms and had been mathematically proven.

Moreover, a quantum algorithm was designed to solve the shortest paths problem between the two points in a network. Another quantum algorithm for a minimum weight spanning tree in the graph was also designed. These quantum algorithms can be applied to solve routing problem in the quantum networks and the quantum multicomputer. The designed hybrid architecture and framework were tested using the above quantum algorithms and the existing quantum algorithms. Implementing and simulating results are then represented based on the probabilistic hybrid algorithm in the case of linear array, binary heap and quantum search for dense and sparse graphs.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

RANGKA PEMPROSESAN KUANTUM DAN ALGORITMA HIBRID UNTUK MASALAH LALUAN

Oleh

MOHAMMAD REZA SOLTAN AGHAEI

Mei 2010

Pengerusi: **Zuriati Bt Ahmad Zukarnain, PhD**

Fakulti: **Sains Komputer dan Teknologi Maklumat**

Teori kompleks kuantum ditubuhkan apabila komputer kuantum menawarkan kelebihan kelajuan pengiraan berbanding komputer klasik . Pada masa ini, hanya beberapa teknik umum yang popular dalam bidang pengkomputeran kuantum dan mencari masalah-masalah kepada kelajuan kuantum adalah amat diutamakan. Walau bagaimanapun, kecekapan algoritma kauntum adalah amat terhad dalam nombor dan skop; tiada penemuan yang nyata dicapai dalam perlaksanaan fisikal. Yang paling penting, algoritma ini masih belum cukup matang untuk digunakan dalam pengkomputeran kuantum.

Unit Pemprosesan Kuantum (UPK) adalah sesuatu pemprosessan komputer kuantum yang mampu untuk melakukan pengiraan kuantum. Satu komponen tipikal dalam UPK adalah alat kuantum yang menjalankan algoritma kuantum; iaitu Unihybridt Pemprosesan Algoritma Kuantum (UPAK). Fokus kajian ini adalah untuk membangunkan satu rangka kerja mengenai UPAK dan algoritma arsitektur untuk algoritma klasik-kuantum. Rangka kerja ini digunakan untuk menambah presestasi perlaksanaan persembahan algoritma kuantum. Rangka kerja menunjukkan hampir

keseluruhan senibina prosesan kuantum berkemampuan melaksanakan Algoritma Kuantum. Secara khususnya, UPAK boleh digunakan sebagai nod kuantum untuk mereka bentuk satu kuantum multikomputer.

Satu platform seragam telah dicadangkan bagi UPAK untuk gunakan dalam kajian ini. Pada mulanya, seni bina hibrid telah direka bentuk untuk algoritma kuantum. Kemudian, hubungan di antara klasik dan bahagian-bahagian algoritma hibrid kuantum telahpun dikeluarkan dan langkah utama algoritma hibrid telahpun ditentukan. Selepas itu, rangka kerja UPAK telah direkabentuk dan dibangunkan. Untuk tujuan ini, sesetengah pintu dan hubungan-hubungan telahpun ditujukan dalam rangka kerja di mana boleh digunakan untuk algoritma kuantum akan datang. Selanjutnya, rangka kerja telah dibina, dilaksanakan and disimulasikan untuk kewujudan algoritma kuantum pada komputer klasik . Keputusan menunjukkan di mana rangka kerja adalah bersesuaian untuk algoritma kuantum dan telah dibuktikan secara metamatik..

Dengan itu, satu algoritma kuantum telah direka bentuk untuk menyelesaikan jalan singkat masalah antara dua titik dalam rangkaian. Algoritma kuantum satu lagi untuk "minimal weight spanning tree" dalam graf juga telah direka bentuk. Algoritma kuantum ini boleh digunakan untuk menyelesaikan masalah laluan dalam rangkain kuantum dan kuantum multikomputer. Rekabentuk seni bina hibrid dan rangka kerja telah pun diuji mengunakan algoritma kuantum di atas dan algoritma kuantum yang ada masa kini. Perlaksanaan dan keputusan simulasi dibentangkan berdasarkan pada algoritma hibrid kebarangkalian dalam kes tatasusunan linear, "binary heap" dan carian kuantum untuk merapatkan ruang graf.

ACKNOWLEDGEMENTS

Thanks to God for everything during my voyage of knowledge exploration. First and foremost, I would like to express my sincere gratitude to my supervisor Dr. Zuriati Ahmad Zukarnain for giving me an opportunity to start off this project. Through the course of my study, I have had the great fortune to get to know and interact with her. Her comments and suggestions for further development as well as her assistance during writing this thesis are invaluable to me. Her talent, diverse background, interest, teaching and research style has provided for me an exceptional opportunity to learn and made be become a better student. I would like to express my sincere thanks and appreciation to the supervisory committee members Associate Professor Dr. Ali Mamat and Associate Professor Dr. Hishamuddin Zainuddin for their guidance, valuable suggestions and advice throughout this work in making this a success.

My deepest appreciation to my wife Ms. Zohre Montazeri and also my kids, who have been very supportive and patiently waiting for me to complete my study.

For the others who have directly or indirectly helped me in the completion of my work, I thank you all.

MOHAMMAD REZA SOLTAN AGHAEI

May 2010

I certify that a Thesis Examination Committee has met on 12 May 2010 to conduct the final examination of **Mohammad Reza Soltan Aghaei** on his thesis entitled **"Quantum Processing Framework and Hybrid Algorithms for Routing Problems"** in accordance with the Universities and University Colleges Act 1971 and Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the degree of Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Mohamed Othman, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Azmi Jafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mohamed Ridza Wahiddin, PhD
Professor
MIMOS Berhad
Technology Park Malaysia
Kuala Lumpur, Malaysia
(External Examiner)

Kwek Leong Chuan, PhD
Associate Professor
Department of Physics, Faculty of Science
National University of Singapore (NUS)
Singapore
(External Examiner)

BUJANG BIN KIM HUAT, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 12 August 2010

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Zuriati Ahmad Zukarnain, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Ali Mamat, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Md. Hishamuddin Zainuddin, PhD
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

____
HASANAH MOHD GHAZALI, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 12 August 2010

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or other institution.

____

MOHAMMAD REZA SOLTAN AGHAEI

Date: 12 May 2010

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CPU	Central Processing Unit
QPU	Quantum Processing Unit
QAPU	Quantum Algorithm Processing Unit
QCPU	Quantum CPU
QFT	Quantum Fourier Transform
QC	Quantum Computer
QEC	Quantum Error Correction
NMR	Nuclear Magnetic Resonance
EPR	Einstein-Podolsky-Rosen
CQED	Cavity Quantum Electro-Dynamics
SQUID	Superconductive Quantum Interference Devices
Bra	Dirac notation for a complex-conjugate row vector: $\langle\psi|$. See also ket.
Decoherence	The degradation of the state of a quantum system as it interacts with its environment in ways that are impossible to adequately characterize; causes errors in qubits.
Diameter	The largest number of hops through the network to get from any node to any other.
Entanglement	The property of two particles with a common origin whereby a measurement on one of the particles determines not only its quantum state but the quantum state of the other particle as well.
Ket	Dirac notation for a column vector: $|\psi\rangle$. For an n-qubit system, consists of 2n entries. See also bra.
Link	A physical connection in a network between two nodes, or a node and a piece of dedicated networking equipment such as a router. May be serial or parallel.
Node	A computational element attached to a network.
Qubit	A two-level quantum system; the basic unit of quantum information. A qubit may be in a superposition of its two states. Qubits may be physical or logical.

Qubus	A system that uses a strong probe beam and weak nonlinearities to entangle two or more qubits over a distance.
Qubyte	Eight qubits.
Separable	Two quantum systems that are not entangled are separable.
Superposition	Is a fundamental property of quantum mechanics and it defines the collection of all possible states that an object can have.
Unitary transform	The most common mathematical representation of a quantum gate; for an n-qubit gate, a $2n \times 2n$ unitary matrix that effects a rotation in the appropriate space. A unitary transform U satisfies the condition that $U^\dagger U = UU^\dagger = I$.

CHAPTER 1

INTRODUCTION

1.1 Motivation and Background

A primary goal of the theory of quantum complexity is to determine when quantum computers may offer a computational speed-up over classical computers. At present, there are only a few general techniques known in the field of quantum computing and finding new problems which give a polynomial time quantum algorithm for some problem for which no classical polynomial time solution is known. The question of which classical algorithms can be sped up by quantum computing is of course a very interesting one. At present, there are a few general techniques known in the field of quantum computing and finding new problems that are amenable to quantum speedups is a high priority. Given the possible power of quantum parallelism, much work has been done to show formally with mathematical proofs how quantum computers differ from classical ones in their power to compute things.

The idea of quantum computer was first explored in the 1970's and early 1980's by physicists and computer scientists such as Charles H. Bennett, Paul A. Benioff (Benioff 1982) and the late Richard P. Feynman (Feynman 1982). The idea emerged when they were pondering the fundamental limits of classical computation. If technology continued to abide by Moore's Law (Moore April 1965), the continually shrinking size of circuits on silicon chips would eventually reach a point where individual elements would be no larger than a few atoms. Here at the atomic scale, quantum mechanical, instead of classical, governs the behavior and properties of the circuit. This then raised the question of whether a new kind of computer could be devised based on the principles of quantum physics.

Feynman produced an abstract model in 1982 that showed how a quantum system which used quantum mechanics intrinsically could be used to do computations and might be more powerful than a classical computer (Feynman 1982). Later, in 1985, Deutsch (Deutsch 1985) realized that Feynman's assertion could eventually lead to a general purpose quantum computer and published a crucial theoretical paper showing that any physical process, in principle, could be modeled perfectly by a quantum computer. Thus, a quantum computer would have capabilities far beyond those of any traditional classical computer. Since then, quantum computing has attracted lots of scientists to study on different directions of this area: quantum algorithms, quantum error correction, quantum encryptions, physical implementations, and so on. Many creative and exciting developments were achieved and quantum computation shows more and more potentials. To date, it is widely believed that if large-scale quantum computer could be built, it would be able to solve certain problems faster than any classical computer, which makes it a possible candidate for the next generation of high-performance computer.

David Deutsch and Richard Jozsa showed in a paper in 1992 that there was an algorithm that could be run in single query on a quantum computer, but required linear time on a deterministic Turing machine (Deutsch and Jozsa 1992). This may have been the first example of a quantum computer being shown to be exponentially faster than a deterministic Turing machine.

One of the most interesting open questions in quantum complexity theory is whether there exists a polynomial time quantum algorithm for solving so-called NP-hard problems. NP-hard problems constitute a class of computational problems that arise frequently in science and engineering. No one has yet found a polynomial time quantum algorithm for solving NP-hard problems, and what evidence there is, is discouraging (Bennett and others 2001). However, there are some exponential time quantum algorithms that run polynomial faster than their closest classical counterparts. Reducing the exponent in an exponential function is not a total victory because the resulting algorithm is still exponential. Nevertheless, it represents a significant speedup.

Peter W. Shor (Shor 1994) in a paper in 1994 showed Shor's Factoring algorithm is a Polynomial Time Algorithm for Prime Factorization and Discrete Logarithms on a Quantum Computer. All known algorithms for factoring an *n*-bit number on a classical computer taken time proportional to $O(2^n)$ time and in the best known algorithm to $O(\exp(n^{1/3}))$ time. But Shor's algorithm for factoring on a quantum computer takes time proportional to $O(n^2 \log(n))$.

L. Grover in 1996 (Grover 1996) developed Quantum search algorithm. Grover's search algorithm can search an unstructured space of N possibilities in $O(\sqrt{N})$ time, and the classical computer can do search on average in $O(N)$. It is sometimes referred to as amplitude amplification and has been found to be useful for quantum counting, and as a wrapper for other algorithms (Brassard, Høyer et al. 1998; Grover 2005). The speedup of Grover's algorithm is achieved by exploiting both quantum parallelism and the fact that in quantum theory a probability is the square of the probability amplitude. Bennett and co-workers (Bennett and others 2001) and Zalka (Zalka 1999) showed that Grover's algorithm is optimal. No classical or quantum algorithm can solve this problem faster than a time of order. Furthermore, other algorithms are Simon's algorithm to finds the hidden string (Simon 1994), Hallgren's algorithm to solve the Pell's equation (Hallgren 2002), or the fascinating topic of quantum random walks (Aharonov, Davidovich et al. 1993; Kempe 2003). Nonetheless, efficient quantum algorithms are very limited in number and scope; no real breakthrough has yet been achieved in physical implementations. Most importantly, these algorithms are not still matured adequately to be applied in real quantum computations. This study has been carried out to design the quantum processor framework of a quantum computer which able to execute the quantum algorithms.

The motivation of this thesis was to continue the research of Van Meter (Van Meter, Nemoto et al. 2006) in designing multicomputer. He proposed the architecture of a quantum multicomputer optimized for running Shor's factoring algorithm (Van Meter, Itoh et al. 2005; Van Meter, Nemoto et al. 2006). The creation of the quantum multicomputer began with the optimization of the quantum modular exponentiation for Shor's factoring algorithm. The algorithm presented by Van meter reduces wall-clock time by a factor of one million for a six-thousand bit number (Van Meter, Itoh et al. 2005). Van Meter described a quantum multicomputer in terms of calculating factoring large number, and this architecture does not comprise other quantum algorithms (Van Meter 2004; Van Meter and Itoh 2005; Van Meter and Oskin 2006). Similarly, he described a linear topology for quantum network, but left research on the hardware requirements of nodes and routing in quantum networks to other researchers. This study has been carried out to design the framework of nodes for multicomputer that runs the available quantum algorithms. The quantum circuit of the node can be applied as a Quantum Algorithm Processing Unit (QAPU) in the processor of a quantum computer. Moreover, a quantum algorithm was also designed for routing in the quantum network.

1.2 Problem Statement

So far, a few efficient quantum algorithms have been introduced. However, there has been no quantum computer to run these algorithms yet, each quantum algorithm has been done mathematically. The execution of the quantum algorithms do by simulation on the classical computer. There is no uniform platform that consists all of them. A quantum processor unit that executes all the quantum algorithms is therefore needed. The quantum processor can be applied as a quantum node in designing multicomputer. Moreover, the quantum algorithms are also known as the hybrid (classical-quantum) algorithms, and thus, a general plan of hybrid algorithms is required to show the interaction between quantum and classical part of hybrid algorithms. According to earlier discussion, this problem can be broken down into the following problems.

- There has been no quantum computer to entirely support quantum algorithms yet.
- There is no uniform platform that supports all of the quantum algorithms.

- A framework of the quantum processor unit that executes all the quantum algorithms is needed.
- A general plan of hybrid (classical-quantum) architecture is required to show the interaction between quantum and classical part of the hybrid algorithms.
- There is no efficient quantum algorithm for the quantum network routing.

The focus of this study was to develop a framework of the quantum processor which can execute the quantum algorithms. This processor can also be applied as a quantum node in the quantum multicomputer. The quantum multicomputer consists of three primary sub-systems, namely the quantum computational node hardware, the quantum interconnection hardware, and the software to run on the system. Interconnect hardware consists of basic link technologies and the manner of assembling a system was one of the contributions by Van Meter's researches (Van Meter 2004; Van Meter and Itoh 2005; Van Meter, Itoh et al. 2005; Van Meter, Nemoto et al. 2006; Van Meter and Oskin 2006). Unfortunately, node hardware and routing problem in the quantum network have not been explored or solved by him, and left these to other researchers. Node architecture is the main contribution of this thesis and finding a quantum algorithm for a network routing is one of its primary contributions.

1.3 Research Objectives

The main objective of this research is to develop a framework of the QAPU and hybrid architecture to execute quantum algorithms. This processor can also be applied as a *node* in a quantum multicomputer or a quantum co-processor in the classical computer which