6COM1046 Quantum Computing

Assignment : Classical and Quantum Applications, Protocols & Complexity

Furkan Kilicaslan

15069985

Tutors :

Joseph Spring

Grant Hubbard

Peter Lane

Table of Contents :

I – Heterogeneity and Examples from Classical Computer Systems, Networks and Distributed Systems

II – Four Different Types Of Quantum Computers and a Debate Over The Existence of Quantum Computers

III – Applications of Quantum Computation and Information

IV – Final Thoughts

I – Heterogeneity and Examples from Classical Computer Systems, Networks and Distributed Systems

Heterogeneous computing refers to computation systems that use multiple types of processors.Such systems improve performance not only by adding pure extra processing power in terms of cores but at the same time implementing unique capabilities to perform specific tasks.Heterogeneous system architecture makes use of multiple types of processors such as CPUs and GPUs to increase overall performance.So that the GPU can focus on 3D rendering and mathematically complex computations on massive data sets while the CPU can run more classical tasks of running the computer and operating the computer system.

Towards the end of 2010, dual-core and quad-core computer processors became much more affordable and popular in the industry.Such multicore processing power came with its own problems.The extra amount of cores and the memory needed, increased processor size and an intense amount of power consumption.During this era the advances in semiconductor technology led to many interesting deveopments in GPUs in terms of complexity and sophistication.GPUs utilize vector processing capabilities which helps them perform parallel computations on massive sets of data and at the same time doing it in much lower consumption of power of course relative to serial processing counterparts.For these reasons having multiple types of processors of the same or different kinds increases overall performance in computation hence the importance of heterogeneity.

A heterogeneous network is a network of connected computers composed from different types of devices or operating systems and/or protocols.Such as networks consisting of computers using Linux, Windows, Android, Ios.Also a wireless network providing services through both wireless LAN and cellular network can be a heterogeneous network.

Heterogeneous wireless networks have multiple benefits over the traditional homogenous wireless networks.These can be increased reliability, coverage and improved spectrum efficiency.

Distributed systems contain multiple types of hardware and software working in coherence in order to solve problems that are served.In the system there can be diverse ways of data representation.Such as different representations of integers, streams, floating point numbers and character sets.Such data can mostly be transfered from one system to another without losing significant data.Still there can be many different sets of instructions for an application and the instructions for an application may not be easily converted for another system.There is no global binary which causes transferring, a difficult process on most computer.No two computer is exactly the same so creating a canonical universal form of instructions is an incredibly challenging problem.Some computers might have different clock cycles, different memory capacities, disk farms, printers and other such accessories.So heterogeneity in distributed systems can cause many problems.

In general heterogeneous computing creates new problems that aren’t present homogeneous systems.As the level of heterogeneity increases in a system there will be non-uniformity in system development, programming practices and overall capability of the system.Computer elements can have different instruction-set architecture, application binary interface, application programming interface, low-level language feature implementations, memory interface and hierarchy, interconnection and performance leading to a diverse range of problems coming along with heterogeneity.

In conclusion heterogeneity is born as a necessity of improved processing and computing power but it brought its own challenges with itself.Solving these problems and improving overall performance of heterogeneous systems is an important field of work in computer science and engineering.

II – Four Different Types Of Quantum Computers and a Debate Over The Existence of Quantum Computers

A quantum computer can be defined as a computing system that can utilize the quantum phenomena based on the sub-atomic particle behaviour to perform calculations in a much more efficient manner than a classical computer that works on binary system.Such a computer can make use of quantum entanglement and most importantly superposition in the form of using quantum bits which is basically a superposition of states.

The idea of a computer system based on the quantum mechanics have been around for longer than one anticipates.Yuri Manin was the first ever to propose a quantum computer system in 1980 with his paper "Computable and Uncomputable".Later on with numerous researchers, engineers and investors realising the potential of quantum computers there have been an increasing amount of work done on this area.Paul Benioff, Richard Feynman, Asher Peres and David Deutsch have come up with many ideas on how to build a quantum computer and they have built possible frameworks for this process.

a) Paul Benioff (1982) have been the first to try and create a Turing machine utilizing quantum mechanics.As can be found on Gruska's(1999) studies, Benioff's quantumized turing machine has a tape consisting of a sequence of quantum bits(spin states).Each of these becoming either of the basis states $|0\rangle\, or|1\rangle$ after each computation steps.In this way he could encode a binary input together with intermediate results.Together with the program to be operated the finite control was incorporated in the Hamiltonian of a very deliberately designed Schrödinger equation.

There was of course problems with Benioff's works.Benioff's quantum computer could utilize qubits, being in a superposition of quantum states while a computation was ongoing but after each of these computations the tape of the machine had to be in a basis state of information such as binary hence the quantum related properties(superposition of basis states, entanglement, paralellism) of the model could not be found. Eventhough his work was based upon quantum mechanics, a classical Turing machine could easily do what he was achieving.

The most significant problem with Benioff's design was that in order to compute anything with his quantumized turing machine the whole set of computation instructions alongside with the program itself had to be fed which meant that in order to design the quantum computer Benioff has designed the solution of the problem had to be known as well.The biggest issue with Benioff's quantum computer implementation was finding a way to conceive the interactions between the head, the quantum bits that may have been far away from each other.

b) Richard Feynman (1982,1986), at a first look approached quantum computing in a simple way.It was based upon the fact that there are universal reversible Boolean gates.His major impact on the field was producing a general method of designing the Hamiltonian for a quantum circuit where each gate in the circuit executes a unitary operation.This at first seemed like a prohibitive approach.In this approach programming actually meant building a new quantum circuit and setting the approppriate inputs for every new design.However due to Yao's(1993) results, it is now fair that from the point of pure computation power this model of quantum circuits have equivalent strength as quantum Turing machines.

Assuming that we have a serial connection of *k* quantum gates in a quantum circuit.Each of these quantum gates performing a unitary operation, $U_1, \dots \dots, U_k$ Feynman managed to prove that the the form a Hamiltonian H should have in the Schrödinger equation for a such quantum circuit.

$$U(t) = e^{-\frac{i}{h}Ht}$$

In this way Feynman has shown a methodical although not an adequate way of transforming a quantum circuit of a quantum computer to the Schrödinger equation which simulates the computation instructions of the circuit.

Feynman has used additional *k* qubits for the "program counter sites" alongside with the "creation" operators $c_i(i = 1, \dots \dots, k)$ and the "annihilation operators" $a_i(i = 0, \dots \dots, k - 1)$ Each of these creation operator c_i "sets the *i*th counter qubit to 1" and the annihilation operator to 0.Then the general Hamiltanion falls into the following form :

$$H = \sum_{i=0}^{k-1} (c_{i+1} \,.\, a_i \,.\, U_{i+1} + (c_{i+1} \,.\, a_i \,.\, U_{i+1})^*)$$

The first term of the equation absolves the sequential execution of all circuit gates.The conjugate terms are needed to be added as well in order to maintain the necessity of the resulting Hamiltanion being Hermitian.Overall, Feynman's approach of quantum computing requires a register of *m* + *k* – *1* qubits in order to handle *k* counters and *m* input quantum bits.More specifically :

$$c = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Computation on a such quantum circuit is initiated by putting input bits into the input register and the pointer to occupy the site 0.Then it is proceeded to check if the site k is empty or the site has any pointer.Once the cursor is found, it is removed to make sure it doesn't return down the program stream.At that moment the register has all the inputs necessary to be measured.Ending the program is not a concern of the quantum computer itself.It is to be decided manually on when to execute the measurement.

In this model Feynmann created, the whole quantum uncertainty of the computation is focused in the time necessary for the computation to be performed and not in the precision of the outcomes.In other words, if a computation is performed and a particular bit shows it, the result is always correct.

c) Most of Asher Peres' (1985) work was improvements on Richard Feynman's and Paul Benioff's ideas on quantum computer design.Peres developed Feynman's quantum computer model in a such manner that the calculation results would appear at the exact time and location.Also Peres fostered the idea of creating a computer with a continuous quantum logic with implementing the superposition phenomena on the basis states.

As is on the preceding attempts of building a quantum computer, Peres's focus is on writing a Hamiltonian H such that the evolution of time $e^{-\frac{iHt}{h}}$ represents the performing of a computation.The major improvement in Peres's models is an analysis of possible errors occurring in the Hamiltanion and in the measurements.Most specifically a concept of quantum error-correcting codes and how to integrate these into Hamiltonian quantum error correction procedures.

Peres dealt with the occassion of one qubit being encoded by three $(|0\rangle \rightarrow |000\rangle, |1\rangle \rightarrow |111\rangle)$ so the possible error states have the form

$$\alpha_0|000\rangle + \beta_0|100\rangle + \gamma_0|010\rangle + \delta_0|001\rangle$$

or

$$\alpha_1|111\rangle + \beta_1|011\rangle + \gamma_1|101\rangle + \delta_1|110\rangle$$

For appropriate amplitudes : $\alpha_i,\ \beta_i,\ \gamma_i,\ \delta_i,\ i = 0{,}1$.

Additionally Peres thought of a way of utilizing Stern-Gerlach magnets in error detection and error correction for quantum computers.Also he recognized that the unitary operations can be used in error correction.Lastly, Peres found ways of integrating error correction in the Hamiltonian so that the error probability could be reduced to an arbitrarily small value.

Peres, in his studies of quantum error correction never used entanglement phenomena to safeguard quantum information which led to his technique being poor.Although it was not good enough to protect quantum information, it was the first ever approach to acknowledge quantum error correcting codes.He also talked about the possibilities of creating a quantum computer with general quantum bit states $\alpha|0\rangle + \beta|1\rangle$.

d) David Deutsch had a basic philosophical stance.It was that underlying the Church – Turing principle there was an implicit phsyical assertion.On this basis he established his own phsyical version of Church – Turing principle : “Every finitely realizable phsyical system can be perfectly simulated by a universal model computing machine operating by finite means.”

David Deutsch (1985) introduced a general, constitutionally new and completely quantum model of quantum computation.In Deutsch’s Turing machine ***U*** the tape (***t***) consists of an infinite sequence of quantum bits and the finite control consists of a finite sequence of quantum bits (***m***).Also there is an observable ***x***, which can have any integer ***Z*** as its potential value which is used as a pointer to the currently scanned tape cell.Deutsch handles the infinitely long tape problem by accepting the tape is not fixed and it can be moved around according to the transmitted signals at a finite speed between bordering divisions by a mechanism.In conclusion the state of the quantum computer ***U*** is a unit vector in the space spanned by the basis vectors : $|\boldsymbol{x}, \boldsymbol{t}, \boldsymbol{m}\rangle$

The dynamics of the Turing machine ***U*** is given by a constant unitary operator **U** and for the evolution of the state $|\Psi(t)\rangle$ it holds

$$|\Psi(t)\rangle = U^t\ |\Psi(0)\rangle\ where\ |\Psi(0)\rangle = \sum_n \lambda_n\ |0,0,\boldsymbol{t}\rangle$$

And only finitely many λ_i are non-zero if an infinite amount of elements in ***t*** are non - zero.**U** has to be able to meet a special condition in order to complete operations “by finite means.”

David Deutsch was conscious of the aspects of quantum computing such as quantum paralellism and entanglement.In order to explain such features he used Everett’s many worlds interpretation as he explains, “The intuitive explanation of these properties places an intolerable strain on all interpretations of quantum theory other than Everett’s.”

In addition David Deutsch portrayed a universal quantum computer capable of simulating every finitely realisable physical system, thus any other possible quantum computer with arbitrarily high correctness.In order to design a such quantum computer Deutsch made use of the fact that if α is any irrational multiple of π, then the following four transformations form a group dense in the group of all unitary transformations in H_2.

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \quad \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix}, \quad \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

According to Michele Mosca, a co-founder of the Institute for Quantum Computing at the University of Waterloo in Canada, the very meaning of the phrase “quantum computer” is fuzzy to begin with.He came up with 5 definitions for the phrase (Actually 5 and a half) :

Definition 1:

Since the world is quantum, any computer is a quantum computer. Conventional computers are just weak quantum computers, since they don’t exploit intrinsically quantum effects, such as superposition and entanglement.

Definition 2:

A quantum computer is a computer that uses intrinsically quantum effects that cannot naturally be modeled by classical physics. Classical computers may be able to mathematically simulate instances of such computers, but they are not implementing the same kinds of quantum operations.

Definition 2’:

Definition 2, where there are strong tests or proofs of the quantum effects at play (e.g. by doing Bell tests).

Definition 3:

A quantum computer is a computer that uses intrinsically quantum effects to gain some advantage over the best known classical algorithms for some problem.

Definition 4:

A quantum computer is a computer that uses intrinsically quantum effects to gain an asymptotic speed-up over the best known classical algorithms for some problem. (The difference with definition 3 is that the advantage is a fundamental algorithmic one that grows for larger instances of the problem; versus advantages more closely tied to hardware or restricted to instances of some bounded size.)

Definition 5:

A quantum computer is a computer that is able to capture the full computational power of quantum mechanics, just as conventional computers are believed to capture the full computational power of classical physics. This means, e.g. that it could implement any quantum algorithm specified in any of the standard quantum computation models. It also means that the device is in principle scalable to large sizes so that larger instances of computational problems may be tackled.

It is very easy to debate over the existence of a quantum computer based on these definitions.There are several existing commercial “so called” quantum computers in the market.D-Wave is the leading company in this market with quantum computers witholding

2000 quantum bits inside and have customers such as; Google, Lockheed Martin and NASA and none of these customers have so far asked for a refund.But going back to the 5 definitions the products of D-Wave’s product is more suitable for the 3rd definition.As a personal opinion, I believe that until we can use quantum computers that fit the fifth definition we are not going to be experiencing a fully quantum machine.

III – Applications of Quantum Computation and Information

a) Quantum cryptography has now proven to cater complete security between two communicating peers.In addition to that the features of quantum properties have the possibility to break classical encryption system such as Data Encryption Standard (DES) and RSA.

Cryptography have quite a long mark on the history line.It dates back to ancient rome such as the implementation of the Caesar cipher which shifts the letter of each message by three letters to create a secret message.Of course this method is very primitive and insecure.In time, techniques of cryptography have improved immensely.These days, in modern times we use keys to encrypt our messages.A simple form of this type of encryption can be given as a code wheel.

Key	A	B	C	D	E	F	A	B	C	D	E	F
Shift By	1	2	3	4	5	6	1	2	3	4	5	6
Message	C	R	Y	P	T	O	G	R	A	P	H	Y
Encoding	D	T	B	T	Y	U	H	T	D	T	M	E

In time these encryption algorithms improved a lot.Codes such as DES, IDEA were put into use with typically 64 and 128 bit secret keys.Also RSA (Public Key Encryption) uses a combination of public and private keys to encrypt data.In a such scenario the public key can encrypt the data but it can not decrypt it.Compiling the private key from the public key requires an immense amount of computation power in classical computers hence keeping the public key encryption safe.

Of course some key schemes are much stronger than the others such as DES and IDEA being stronger than the Caeser cipher codes.The most powerful key code in use today is a one – time use PAD.This key is sent to each side of the communication and used only once for encryption and decryption.This method have a downside of course as an eavesdropper can be easily listening on the transmission and acquire the PAD.Quantum key distribution handles such problems with a completely secure key distribution.

In todays public key encryption algorithms “trap door function” system is in use which is based on some mathematical assumptions, especially the ones that are difficult to factorise for large integers.As Shor’s algorithm shows this encryption method is now in danger.

The major aspect of quantum cryptography is that it provides a completely secure data transfer.The first time a successful quantum device used on cryptographic purposes was tested in 1989 by C. H. Bennet and G. Brassard [Castro, M. 1997].This device had the ability of translating a code over 30 centimeters utilizing polarised light, calcite crystals and numerous other electro-optical devices.Such a type of cryptography relies on quantum effects rather than the classical trap door function.

Also secure communication channels can be provided with use of quantum key distribution since quantum cryptography utilizes quantum phenomena it is possible to tell if an eavesdropper have been listening on the channel by checking error - rates.

Since the idea of quantum computing have surfaced there have been multiple approaches to create quantum algorithms which is a method to combine unitary operations in a quantum system in order to accomplish some specific computational objective.Such algorithms give an edge over their classical system counterparts.

For example Shor's algorithm(1995) reduces the time complexity of factorisation of arbitrarily big numbers down to $O((log\,N)^3)$ where the classical counterpart algorithm has a complexity of exponential.Shor's algorithm poses a big threat to cryptography especially public key encryption where RSA relies on the computational power needed to factorise large integers.As another example Grover's database search algorithm again caters a quadratic boost of searching a linear list of *N* items.Most of the other quantum algorithms have similarities with these two algorithms or are based on these.

b) David Deutsch have discovered a problem that can be solved faster in quantum computers than it can be solved in traditional computers.Although this problem is not an important computer science problem it is crucial in seeing how quantum computers can be implemented.

The main problem is as following.We suppose we have a function *f* which maps {0,1} into {0,1} and we want to learn if this function is one to one or not.This problem can be solved in traditional computers by working out *f(0) XOR f(1).*If the function is one to one it will be evaluated to 1, otherwise to 0.In traditional computers the function has to be evaluated twice to obtain a result while Deutsch's algorithm in a quantum computer only evaluates the function once using Hadamard transformations.

Deutsch – Jozsa algorithm is an improvement over the original Deutsch algorithm.Eventhough it has almost no practical use, it displays one of the first ever examples of quantum computing which is exponentially faster than any traditional algorithm.The important difference between the Deutsch's algorithm is Deutsch – Jozsa algorithm can evaluate multiple quantum bits in one operation.The main problem that is addressed in Deutsch – Jozsa algorithm is to learn if a function *f* is constant for all inputs or if it is balanced.

c) One of the most significant, motivating and extraordinary results obtained in quantum computing is the Shor's algorithm that provides polynomial time for factorization and computation of discrete logarithms.Peter Shor, having inspired by Simon(1994) have gathered some ideas about getting approximations of the period and extracting the exact period cleverly using Quantum Fourier Transformation (QFT).

- Factorization of integers can be reduced to the problem of finding the period of a function
- Fourier transform puts the period of any periodic function into multiples of the reciprocal of the period

Also Shor managed to display that all these can be done in an efficient way.The modern cryptographic methods for public key encryption and digital signatures are heavily relying on the fact that there are no existant potent algorithms for integer factorization or computation of discrete logarithms.Manufacturing a quantum computer that can perform the factorization and discrete logarithm implementations of Shor's algorithm would crush the existant reliable cyber security systems.This potential have sparked interest from even outside science and technology field due to the fact that it can create a hole in the current secure systems of banks, corporations and numerous entities relying on public key encryption.Although Shor's algorithm has scared many in its potential, modern cryptography still stand together as the progress of the design of a such quantum computer is very slow.

d) Another important progress in the field of quantum algorithms was by Grover(1996).Grover displayed a quantum method that can be practiced on a complete class of problems where it is hard to find a solution but easy to check a “to – be solution”.Grover’s method of quantum searching and its variations show that quantum computers are faster than traditional computers for problems with a known lower bound of efficiency.

As can be found on Gruska’s work on Quantum Computing(1999) Grover’s quantum algorithm can easily retrieve an item that satisfies a given condition from an unsorted list of *N* items.With the assumption of function $f\colon\{0,1\}^n \rightarrow \{0,1\}$ is given as a black box such that $f(x_0) = 1$ for a single x_0 we can breakdown the algorithm to 5 steps

1. Apply Hadamard transformation H_n in order to make the state
$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\phi\rangle$$
2. Apply the sign-changing operator $v_f\ to\ |\phi\rangle$ in order to create
$$|\varphi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle$$
3. Apply the inversion about average operator $D_n = -H_n R_n^1 H_n$.
4. Repeat $\left[\frac{\pi}{4}\sqrt{2^n}\right]$ times step 2 and step 3.
5. Measure the *x* - register to get x_0 . If $f(x_0) \neq 1$ then go to step 1.

IV – Final Thoughts

As I approach the end of this paper I would like to express some of my feelings and thoughts on this subject.It is quite unorthodox to express feelings in a paper about a science topic but I believe that it is important to go out of the template once in a while to bring a new perspective to the topic and stand out of the crowd.

I was very excited about quantum computing before I took this course.As I have moved through the course, the applications, foundations and importance of the subject such as the Shor’s and Grover’s algorithms’ potentials proved the point of my excitement.Although there have been complications that killed my excitement later on.Quantum phenomena is so unusal and groundbreaking in its properties that it is incredibly hard to grasp even the most fundamental topics about it.You can see this effect even on the researchers studying the topic, personally stating that they don’t understand some aspects of their studies.This can easily break ones motivation.

I will finish my thoughts about quantum computing and the education i have obtained with an analogy.The bananas we eat today are the result of years of selective breeding from their ancestors which had big seeds in them (Wild bananas) causing them to be inedible.Quantum computing at the time being is on its wild form.I have believed that it was edible and tried to eat it but quantum computing still needs years of selective breeding in order to become edible.

Bibliography:

- AMD (2017) What is Heterogeneous Computing? Retrieved From : http://developer.amd.com/resources/heterogeneous-computing/what-is-heterogeneous-computing/
- Heterogeneous network. (2017, January 12). In Wikipedia, The Free Encyclopedia. Retrieved 15:46, April 21, 2017, from https://en.wikipedia.org/w/index.php?title=Heterogeneous_network&oldid=759648295
- Heterogeneous Systems Ronald LeRoi Burback 1998-12-16
- A. Galindo & M.A. Martin-Delgado (2002). Information and Computation: Classical and Quantum Aspects. Universidad Complutense,28040 Madrid, Spain
- J. Gruska (1999). Quantum Computing. Cambridge : University Press
- Riley T. Perry (2010). The Temple of Quantum Computing
- Why nobody can tell whether the world's biggest quantum computer is a quantum computer.(2014) Quartz Media. Retrieved from : https://qz.com/194738
- Deutsch's Algorithm Retrieved From: http://www.cs.xu.edu/~kinne/quantum/deutche.html