วงจรเปรียบเทียบแบบควอนตัมสำหรับควอนตัมคอมพิวเตอร์ชนิดตัวนำยิ่งยวด

นายนภันต์ เบญจสัตตบุษย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2562

QUANTUM COMPARATOR CIRCUIT ON SUPERCONDUCTING QUANTUM COMPUTER

Mr. Naphan Benchasattabuse

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering Program in Computer Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2019

Thesis Title	QUANTUM COMPARATOR CIRCUIT ON SUPERCONDUCTING QUANTUM COMPUTER
By	Mr. Naphan Benchasattabuse
Field of Study	Computer Engineering
Thesis Advisor	Professor Prabhas Chongstitvatana, Ph.D.

Accepted by the Faculty of Engineering, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

..... Dean of the Faculty of Engineering

(Professor Supot Teachavorasinskun, D.Eng.)

THESIS COMMITTEE

..... Chairman

(Associate Professor Somchai Prasitjutrakul, Ph.D.)

..... Thesis Advisor

(Professor Prabhas Chongstitvatana, Ph.D.)

..... External Examiner

(Assistant Professor Yodthong Rodkaew, Ph.D.)

นภันต์ เบญจสัตตบุษย์: วงจรเปรียบเทียบแบบควอนตัมสำหรับควอนตัมคอมพิวเตอร์ชนิดตัวนำยิ่งยวด. (QUANTUM COMPARATOR CIRCUIT ON SUPER-CONDUCTING QUANTUM COMPUTER) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : ศ. ดร.ประภาส จงสถิตย์วัฒนา, 60 หน้า.

วิทยานิพนธ์เล่มนี้นำเสนอวงจรเปรียบเทียบเชิงควอนตัมที่ถูกปรับปรุงจากวงจรบวกการทดแบบริปเปอร์เชิงควอนตัมของ Cuccaro โดยใช้วิธีการปรับปรุงเกต Toffoli ด้วยวิธีการใช้เฟสเกี่ยวเนื่อง การเปรียบเทียบคุณภาพของวรจรถูกเปรียบเทียบโดยการเทียบค่า Qiskit cost แทนที่การใช้ค่าเปรียบเทียบแบบปกติที่นับจำนวนเกต C-Not และ Toffoli เพียงอย่างเดียว การประเมินวงจรที่นำเสนอกับวงจรเปรียบเทียบอื่นที่เคยมีมาทำโดยการแปลงวงจรอื่นให้อยู่ในรูปพื้นฐานที่สามารถนำไปใช้ได้บนควอนตัมคอมพิวเตอร์ชนิดตัวนำยิ่งยวดโดยจะนำเสนอความแตกต่างระหว่างจำนวนเกตและความลึกของวงจร

ภาควิชา	วิศวกรรมคอมพิวเตอร์	ลายมือชื่อนิสิต	.....
สาขาวิชา	วิศวกรรมคอมพิวเตอร์	ลายมือชื่อ อ.ที่ปรึกษาหลัก	.....
ปีการศึกษา	2562		

6070229621: MAJOR COMPUTER ENGINEERING

KEYWORDS: QUANTUM COMPARATOR / QUANTUM CIRCUIT / QUANTUM ALGORITHM / QUANTUM COMPUTING / QUANTUM CIRCUIT OPTIMIZATION / QUANTUM ARITHMETIC

NAPHAN BENCHASATTABUSE : QUANTUM COMPARATOR CIRCUIT ON SUPERCONDUCTING QUANTUM COMPUTER. ADVISOR : PROF. PRABHAS CHONGSTITVATANA, Ph.D., 60 pp.

In this thesis, we present an optimised quantum comparator circuit based on Cuccaro's ripple-carry quantum adder using relative phase techniques from Maslov's multiple control Toffoli optimisation. We extend the cost function from simply counting C-Not and Toffoli gate to Qiskit cost which defines arbitrary single qubit gate cost as unity and C-Not as the only two qubit gate cost as ten. We report the comparison result between our comparator circuit with previous comparator circuits from literature using optimal Toffoli implementation with Qiskit cost, C-Not count, and circuit depth. We also report our experiment of implementing a two-bit comparator on IBM QX devices.

Department:	Computer Engineering	Student's Signature	.....
Field of Study:	Computer Engineering	Advisor's Signature	.....
Academic Year:	2019		

Acknowledgements

I would like to thank Professor Prabhas Chongstitvatana, my advisor, for driving me into the quantum computing field and inviting me to enter graduate school. Even when I find myself stuck with the difficulty of understanding the theory behind quantum computing or stuck with my research ideas, he always know what to say to cheer people up and give motivations. His ideas on research is extremely intriguing and his guidance on how to do research in broad range of field with novelty is exceptional. Talking with him can spanned for hours but what we students get from his casual talk is not only about research and academic but it comprised of how to lead one's life, negotiation teaching, marketing teaching, how to stay unique, and how to change thinking perspective to fit each environment which are all valuable life lessons.

I thanked my beloved mother who was also another person to pushed me into higher education and always encourage me to stick with the research and for always listening to every complaints and problems on my research.

I also thanked my ISL lab mates in helping with the complex process of doing things inside the university, for exchanging ideas, and constant words of encouragements.

CONTENTS

Page

Abstract (Thai) . . . . . **iv**

Abstract (English) . . . . . **v**

Acknowledgements . . . . . **vi**

Contents . . . . . **vii**

List of Tables . . . . . **ix**

List of Figures . . . . . **x**

1 Introduction **1**

1.1 Quantum Computing Overview 1

1.2 Problem Statement 4

1.3 Thesis Questions 5

1.4 Scope of Work 5

1.5 Research Implication 5

2 Background **7**

2.1 Quantum Basics 7

2.2 Noisy Intermediate Scaled Quantum-Technology Devices 15

2.3 Error Mitigation and Correction 17

2.4 Quality Metric of Quantum Circuit 19

3 Review of Literature **23**

3.1 Adder inspired by classical reversible circuit 23

3.2 Adder using Quantum Fourier Transform 24

3.3 Quantum Comparator 25

3.4 Multiple Controlled Toffoli Gate 25

4 Proposed Circuit 27

5 Results 30

6 Discussion 33

6.1 Summary of Findings 33

6.2 Future Work 34

6.3 Open Problems 34

References 35

Biography 50

LIST OF TABLES

Table **Page**

5.1 Circuit cost summary 30

LIST OF FIGURES

Figure **Page**

2.1 Bloch sphere representation of a qubit 12
2.2 Circuit model of half adder (adding 0 with 1) 13
2.3 Physical connectivity of ibmq_16_melbourne 17
4.1 majority gate (MAJ) 27
4.2 quantum comparator based on Cuccaro adder 28
4.3 Margolous gate 28
4.4 reverse majority gate (RMAJ) 28
5.1 Proposed circuit result from ibmq_vigo 31
5.2 Proposed circuit result from ibmq_ourense 31
5.3 Proposed circuit result from ibmqx2 32

Chapter I

INTRODUCTION

1.1 Quantum Computing Overview

Recently quantum technologies especially quantum computing has been the topic of interest for the general public and researchers. Quantum computing is not exactly new, and the idea of using quantum mechanics to build computer has been around since the 1980s. The problem of simulating quantum systems has always been hard for computers and in the 1980s Richard Feynman, a great physicist of the time, proposed that to simulate a quantum system, it should be easier to just simulate it on another quantum system (Feynman, 1982). David Deutsch, also a physicist, around the same time was trying to find the limit of Church-Turing thesis. Since the underlying principle of the Church-Turing thesis is the *physical realisable machine*, Deutsch looked into the physical aspect of it. He looked into the foundation of all physics, quantum mechanics, and formulate his idea on building computer using quantum mechanics as basis of the computation (Deutsch, 1985).

While trying to prove that quantum computer is more powerful than classical computers. Deutsch came up with a problem, although not a practical one, in which a quantum computer can solve in constant time while classical computer would take linear time to solve (Deutsch and Jozsa, 1992). Later, Bernstein and Vazirani also came up another toy problem that a quantum computer can solve faster than classical (Bernstein and Vazirani, 1997) and then Simon (Simon, 1997) in which his algorithm was actually the first algorithm to move away from binary function and strongly showed that quantum computer is in fact superior to classical computers for certain class of problems. Inspired by Simon's algorithm, Peter Shor in 1994 discovered integer factoring algorithm and discrete logarithm finding (Shor, 1997). The first quantum algorithm able to solve practical real world problem which is believed

to be unsolvable on classical computers. Kitaev later generalised Shor's algorithm and Deutsch-Jozsa's algorithm into algorithm for solving Abelian stabiliser problem (Kitaev, 1995). Quantum search algorithm, an unstructured search algorithm or informally quantum brute-force search, was discovered by Grover in 1996 (Grover, 1997). But after important algorithms like Shor's factoring and Grover's algorithm, not many interesting algorithms were proposed since quantum way of thinking is unnatural. A new development on perspective to quantum view of thinking is needed in order to discover more useful algorithms. Although the progress on quantum algorithm didn't move fast forward during the 1990s, progress were made on the analysis on what ideal quantum computer can and cannot do (Boyer et al., 1998; Bennett et al., 1997; Brassard et al., 2002; Terhal and DiVincenzo, 2004).

Since then, deeper understanding of the nature of quantum algorithm were made (Aaronson, 2013; Aaronson and Ambainis, 2014; Aaronson, 2010) and multiple quantum algorithms were discovered for broader range of topics. Improvements were made on Deutsch-Jozsa algorithm (Myers et al., 2001), Solovay-Kitaev algorithm (Dawson and Nielsen, 2006), and Shor's algorithm (Zalka, 2006). Algorithm for solving systems of linear equations were proposed by Harrow, Hassidim, and Lloyd (Harrow et al., 2009) (HHL algorithm). Multiple applications of HHL algorithm were proposed such as quantum machine learning (Biamonte et al., 2017; Kerenidis and Prakash, 2017). Quantum machine learning is discussed in more detail in (Aaronson, 2014; Mitarai et al., 2018). More about quantum algorithms can be found in (Harrow and Montanaro, 2017; Montanaro, 2016). In addition to quantum algorithms, quantum communication and cryptography also got more advanced with better Quantum Key Distribution algorithm (QKD) (Blundo et al., 2004; Alléaume et al., 2014) and how to increase the distance for quantum communication (Muralidharan et al., 2016).

Recently there has been progress in the making of usable universal quantum computer. In the quest to build a quantum computer, multiple approaches and technologies are used, such as optical system (Qiang et al., 2018), superconducting pro-

cessor (Reagor et al., 2018; Arute et al., 2019), ion-trapped system (Wright et al., 2019), nuclear magnetic resonance (NMR) (Jones, 2001), or silicon chips (Watson et al., 2018). Each technology has its pros and cons in realising a workable quantum computer with a large enough size. The main problem in realising qubits, the basic component of the quantum computer which is analogous to the classical bit, is to maintain the state of qubit long enough to carry out computation. Not only that but the qubit must maintain its quantum effect throughout the computation process, it needs to be tolerant to noises.

Noisy Intermediate Scale Quantum technologies (NISQ), a term coined by John Preskill from Caltech (Preskill, 2018, 2012) (also the person who coined the term Quantum Supremacy). In this NISQ-era, practical applications must be noise resilient. Studies on useful applications in near future of NISQ-era can be found in (Aaronson and Chen, 2017).

One immediate useful application in NISQ-era right now is certifiable random number generator (Brakerski et al., 2018). Another interesting useful application in NISQ-era are variational algorithms. Initially designed for solving quantum chemistry problem; variational quantum algorithm, a hybrid algorithm combining conventional processor and current noisy quantum processor, received a lot of attention currently. By running shallow depth quantum circuits with tunable parameters and using classical optimiser to tune these parameters, variational algorithms can be used to solve optimisation problems. Algorithms that put forth this field were Variational Quantum Eigensolver (VQE) (Peruzzo et al., 2014) and Quantum Approximate Optimisation Algorithm (QAOA) (Farhi et al., 2014). Many applications and variations of VQE and QAOA were proposed in multiple works (McClean et al., 2016; Bravo-Prieto et al., 2019) and sample implementation of solving optimisation problems such as max-cut, travelling salesperson problem, or graph colouring were done in (Koller et al., 2019).

1.2 Problem Statement

Many literature on quantum algorithm assume that the oracle or quantum circuit can be built using mathematical proof but don't state how to actually implement the circuit. Also with the access to quantum computer cloud platform such as from IBM or Rigetti, we want to try realising the quantum algorithm that we've seen in literature on real devices. These public access devices can help us gain insights to discover more useful algorithm to solve interesting problems that we currently have like improving machine learning, decrypting messages, or simulating complex structure of quantum systems. The currently available quantum computer with 14-20 qubits is large enough to solve some of those interesting problems with small input size.

However, fidelity of current public accessible superconducting quantum computers are still under error correcting threshold. Long and complex computation suffers from noises, short decoherence time (T1 $\sim$ 90-100μs; T2 $\sim$ 50-80μs), and gate error ($\sim 0.05\%$ for single qubit gate; $\sim 1\%$ for C-Not gate). Most algorithms developed to solve real-world or interesting problems are often limited by circuit depth, the number of gates which can be performed on qubits before computation outcome is dominated by noise. To address this problem, there are three approaches; by improving hardware resulting in higher gate fidelity, by optimising circuit reducing gate count (especially C-Not or C-Z), and by introducing new native operations to real hardware (such as native swap gate in two microwave pulses instead of using 3 C-Not resulting six pulses).

We are interested in the second approach, on how to optimise circuit from the device-user side. We want to know whether quantum comparator circuit, small but commonly used subroutine for arithmetic based algorithm, can be optimised further and whether its depth is shallow enough to be used to solve optimisation problem with Grover's algorithm. Instead of the popular circuit cost function of using C-Not count or T gate count, we choose Qiskit cost (IBM Q defined cost) as our circuit

cost function to be optimised as most superconducting technology still has single qubit gate error (although one magnitude lower than two-qubit gate) and usually has only one native two-qubit gate (either C-Not, C-Z, or iSwap). To make our design general without restricting to certain devices physical structure, we assume backend to have all-to-all physical connectivity and only suggest ideas on how to modify the design to better match device backend when physical connectivity is known.

1.3 Thesis Questions

1. Assuming all-to-all connectivity, what is a good design for quantum comparator circuit?
2. Can 3-bit quantum comparator be implemented on IBM QX devices with tolerable error?

1.4 Scope of Work

- Circuit cost to compare will assume all-to-all connectivity.
- Circuit cost to compare will only include C-Not count and Qiskit cost.
- Real device experiment will be done on IBM QX only.
- Only one iteration of Grover's algorithm will be used to test quantum comparator usage on real device.

1.5 Research Implication

Giving an example on how to optimise small quantum circuit, in this case quantum comparator, can give more insights and general idea on optimising larger and more complex circuits. For near term noisy devices with longer decoherence

time, lower error rate, and more qubits; instead of only waiting for the improvement on hardware alone, circuit optimisation scheme can help shorten the gap of realisable algorithms on current devices and algorithm for fault tolerant quantum computer. Experimenting with basic component of binary arithmetic such as quantum comparator unit can give us more info on how to devise algorithms for near term devices. If the proposed circuit can be run on real devices and have good correlation of ideal state and real state, then it implies that variational algorithms can incorporate small scale exact circuit to speed up even more.

Chapter II

BACKGROUND

2.1 Quantum Basics

The basics of quantum computing will be briefly discussed in this section, most of the topics are selected from the quantum computing textbook from Nielson and Chuang (Nielsen and Chuang, 2010).

Quantum Bits

Qubit is the fundamental component of computation in quantum computing. It is analogous to classical bit in current computers. Classical bits can hold value of 0 or 1 at a time. Qubits on the other hand, can hold both 0 and 1 at the same time but when observed (or measured) will collapse to being only 0 or 1 like classical bits. a qubit can be described using equation

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

where α and β is a complex number with constraints of

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.2}$$

$|\psi\rangle$ represents the state of this single qubit. $|0\rangle$ and $|1\rangle$ can be thought of as a fancy notation for classical bit 0 and 1 respectively. α and β which we call amplitude can be thought of as a number describing how much 0 or 1 this single qubit is. $||\alpha||^2$ represents the probability that when observed the qubit will act as it has been $|0\rangle$ all along and similarly $||\beta||^2$ for $|1\rangle$. The equation can be understood better with linear algebra, thinking of $|0\rangle$ and $|1\rangle$ as basis in a 2-dimensional complex vector space. A single qubit $|\psi\rangle$ is just a unit vector in the space spanned by the bases thus we can describe a single qubit using 2 complex numbers.

We do not normally use single bit or qubit in our computation but rather a set of bits or qubits (although there is a model of quantum computer with which focuses on single qubit, *deterministic quantum computation with one qubit*(Knill and Laflamme, 1998; Hor-Meyll et al., 2015; Fujii et al., 2018) which we will not talk about it here). In the case of classical bits, suppose we have a n-bit register which can be described using n bit of information. The register can hold 2^n information which then got encoded to represent something in our computation. For the case of qubits, let's look at a system of 2 qubits first which can be represented by

$$|\psi\rangle = (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \tag{2.3}$$

$$|\psi\rangle = \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \alpha_2\beta_1 |10\rangle + \beta_1\beta_2 |11\rangle \tag{2.4}$$

So to think of a quantum system of 2 qubits in terms of linear algebra, the system is a 4-dimensional vector space spanned by 4 bases; $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Similarly for 3-qubit system, the space is spanned by 8 bases; $|000\rangle$, $|001\rangle$, $|010\rangle$, to $|111\rangle$. In general, a system of n qubits can be represented by

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes \cdots \otimes |\psi_n\rangle \tag{2.5}$$

which needs 2^n complex number to describe. This means that we can store much more information compare to classical systems. Do noted that even if we store so much information in the system, when we observe the system to bring out information we still can only see n bits of information. This is the pitfall many fall into thinking when first learning quantum computing. Quantum system can store and compute (which will be discussed in later part) many information at the same time but it tells us very little, storing 2^n but only tell us n. So in order to carry out *fast computation* we need to extract n bits of information which is meaningful to us.

Superposition and Entanglement

The phenomenon of being both 0 and 1 at the same time of qubit is called "superposition". Let us take a step back a bit. Remember that for a n-dimensional vector space, the set of n independent vectors that span the space is called basis. For

a non-trivial vector space, there are infinite set of n vectors that form basis set. So for 2-qubit system, $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ is just one of infinitely many bases we can choose from. We refer to this set of basis as the computational basis. A single qubit can be in a superposition of some basis or just a definite state of another basis. For example,

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2.6}$$

is a superposition in computational basis but a definite state in $(|0\rangle + |1\rangle)$ and $(|0\rangle - |1\rangle)$ basis. Another phenomenon which is important in quantum computation is "entanglement". Entanglement is a phenomenon in which two or more particles (in this case qubits) cannot be described individually. A good example of an entangled state is

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{2.7}$$

The state above is in entangled because the system (2-qubit system) cannot be described via what state each qubit is in but rather it needs to be described as a whole system. It's easier to see from the linear algebra point of view, since we cannot describe a vector in the space using one basis but a combination of basis.

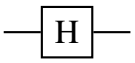
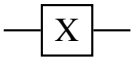
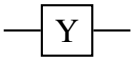
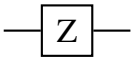
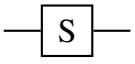
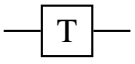
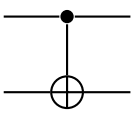
Quantum Computation

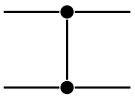
Operations acting on qubits which change the states they are in into some other states are referred to as quantum gate. Quantum gate is not a physical gate like in classical computer but it refers to the manipulation we done on the states which differs for each backend technology; refraction glass in optical technologies, wave pulse in superconducting technologies, or laser beams in ion-trap system. Every computation in quantum computation needs to be reversible except those that destroy superposition such as measurements. In terms of linear algebra, we can think of qubit state as column vector and these operations as unitary matrices or unitary transformations on vectors. Since they're linear transformation, each operation acts on all of the states at the same time. This is what makes quantum computing more powerful than classical computing.

One important fact about quantum computations, even though we can manipulate all the states at the same time, we still need ingenuity to manipulate them in a way that after we finish those operations and extract the information from the 2^{2^n} possible states, we can only get **n meaningful bits** of information.

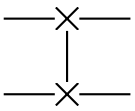
Example of quantum gates

Some selected examples of common gates and circuit symbols used in quantum computing are listed below. Each gate is listed with its circuit model representation (which will be discussed later), name, matrix representation or a brief description of what it does.

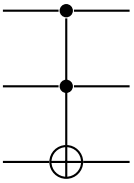
Hadamard		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y		$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z		$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase		$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$		$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$
controlled-Not		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

controlled-Z 

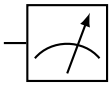
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

swap 

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Toffoli 

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

measurement  Projection onto $|0\rangle$ and $|1\rangle$

qubit wire carrying a single qubit

classical bit wire carrying a classical bit

Visualisation of Qubits

Single Qubit Visualisation

Recall that qubit can be expressed as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and from probability preservation $|\alpha|^2 + |\beta|^2 = 1$, thus the equation describing a single qubit can be

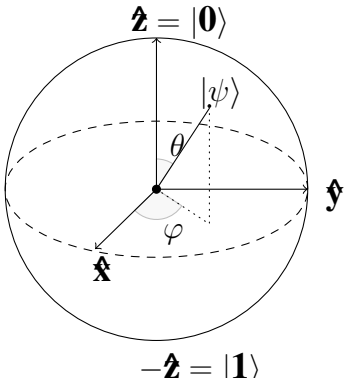


Figure 2.1: Bloch sphere representation of a qubit

rewritten as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right). \tag{2.8}$$

Observed that in this form θ and γ are angles describing a unit vector in a three-dimensional sphere as shown in Figure2.1. This unit sphere is often referred to as *Bloch sphere*. Its visualisation helps us a lot when thinking and reasoning what the state a qubit is in. Now that we have Bloch sphere, how do we translate single qubit gate operations into this representation? Recall that single qubit gates can be expressed as unitary matrices, using a little bit of math, we can see that every single qubit gate maps nicely to a rotation around some axis in this Bloch sphere. Thus we can describe a single qubit gate using three real values; two for defining rotation axis and one for rotation angle.

Multiple Qubit Visualisation

Unfortunately, the Bloch sphere representation does not extend to multiple qubits. There are multiple proposals for visualising multiple qubits states but none of them really receive much popularity since it does not help us much to gain more understanding, so people still using math equation when talking about multiple qubits states.

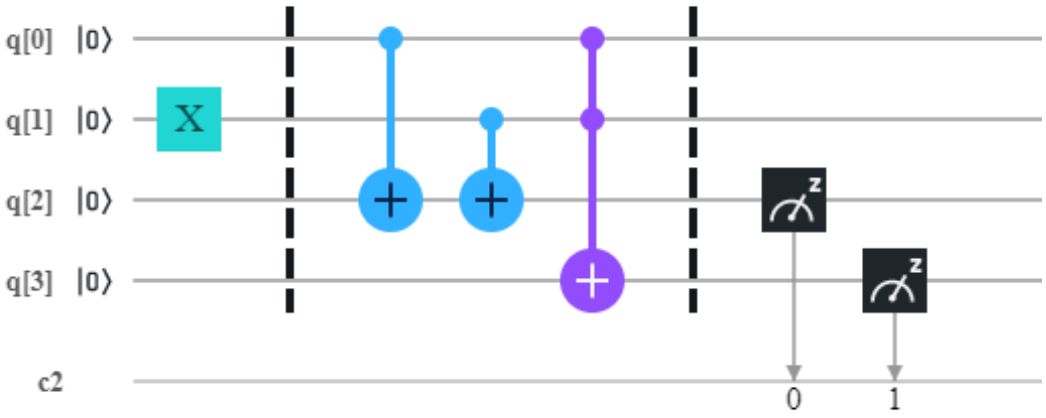


Figure 2.2: Circuit model of half adder (adding 0 with 1)

Circuit Model

To represent quantum program or algorithm, we use circuit model to describe the process of what operations to apply to each qubit. Figure 2.2 is an example of circuit model of half adder with input $|0\rangle$ and $|1\rangle$. Each wire in the circuit model represents each qubit, unless noted otherwise all qubits are initialised in $|0\rangle$ state. Wire with two lines represents classical bit. Box on each qubit wire refers to the operation or quantum gate acting on the qubit. Time goes from left to right, each gate in the same layer refers to the same time slice that it operates on.

Do note that this is circuit model is not a real hardware circuit but is only a way to represent quantum programs similar to how music score is used to represent what each note in the piece should be played but is not limit the music instrument that the piece can be played with.

Quantum Algorithm

Algorithm in quantum computing can be categorised in three broad categories.

Fourier Transform based algorithm - these include Shor's factoring and discrete logarithm algorithm (Shor, 1997), Deutsch-Jozsa (Myers et al., 2001), Simon's (Simon, 1997), any many others. This type of algorithm apply Fourier trans-

form to multiple expanded states and with ingenuity manipulate those states to extract information in some ways that is enough to giveaway the answers without the need to look at the whole states. This type of method is generalised by discovery by Kitaev (Kitaev, 1995) during his attempt to solve Abelian Stabilizer problem and the generalisation to the hidden subgroup problem. The Deutsch-Jozsa algorithm, Shor's algorithm and other related exponentially fast algorithm can be viewed as a special case of Kitaev's algorithm.

Quantum Search Algorithms - This class of algorithm and its basic principles were first discovered by Grover with his famous unstructured search algorithm (Grover, 1997), the quantum version of brute-force searching. Using a technique called amplitude amplification at its core, this type of algorithm was further studied and proved by BBHT (Boyer et al., 1998) that this search type algorithm cannot achieve exponential speed up over classical algorithm and that problem's structure is required to really design an efficient algorithm even for quantum computers.

Quantum Simulation - Simulating quantum systems is hard for classical computers and thus Richard Feynman proposed the idea (Feynman, 1982) that we need new computing model which uses quantum mechanics as the basis to efficiently simulate them. Recently this type of algorithm gained popularity since some Hamiltonian, a physical method to describe energy level of a quantum system, of some easy quantum systems can be implemented on current device of quantum computer and are robust to noises. By reducing problems to quantum systems with known Hamiltonian, many optimisation problems can be done on quantum computers (Peruzzo et al., 2014; Farhi et al., 2014). The problem with current quantum computer will be discussed in the next section and we'll see why this type of algorithm are widely studied right now.

2.2 Noisy Intermediate Scaled Quantum-Technology Devices

At the time of writing, general-purpose error free or fault tolerant quantum computer is yet to be realised. All quantum computers to date possess small number of qubits and are prone to some types of errors or noises which interferes with quantum states of qubits. This type of quantum computer are called Noisy Intermediate Scaled Quantum (NISQ) Computer a term which was coined by John Preskill (Preskill, 2018). The interference from noises make qubits loses their superposition state and the entanglement between qubits which is the key behind power of quantum computer and thus method on fighting against noises is being an active research at the moment.

Noise In NISQ

For each type of NISQ devices, the source and impact of noise varies. For this thesis, only the noise from superconducting technology will be described.

Decoherence

A phenomenon in which qubit loses its quantum mechanical properties, such as losing its superposition states or the entangled states between qubits are called decoherence. In superconducting qubits, there are two sources for decoherence; namely relaxation time (T1) and dephasing time (T2). Relaxation is the energy decay which makes the qubit loses its $|1\rangle$ component and slowly moves to $|0\rangle$. Relaxation time is the in which a pure $|0\rangle$ states lose all of its energy and becomes $|0\rangle$ state. Dephasing is the event that qubit slowly loses its phase, or in the abstract view the complex component of the amplitude. Similarly dephasing time refers to the time duration for a qubit to completely lose its phase component. The study to increase decoherence time and prevent outside causes perturbation are studied in (Ithier et al., 2005). This decoherence time also limits the depth of circuit, how many operations can be done before qubits lose their quantum mechanical proper-

ties, which make long algorithm unrealisable on current NISQ devices.

Gate Error

Quantum computation or qubit manipulation in superconducting devices are performed via microwave pulses. The pulses change qubit's energy level and how it interacts with each other. Controlling exact energy to transfer into qubit is a hard feat and thus there are margin of errors to the expected energy level which can make computation output suffers from some errors. This error occurring when manipulating qubits are called gate errors. Different elementary gates, native gates that each device can perform, have different amounts of errors which will be discussed in more detail in quality metric section. At the time of writing, gate error dominates every other error and is the factor that determines whether a certain algorithm can be run on a certain devices.

Read Out Error

After computation is done, we need to read the output from our quantum computers. At the time of writing even this step has errors. To extract output or calculation results from quantum computers in the case of superconducting devices, another set microwave pulses are applied which in turn introduce another error to our results. Fortunately this type of errors can be mitigated easily.

Physical Connectivity

One important quality of quantum computers are physical connectivity. In order to fully exploit the power of quantum computers entangled qubits are crucial but there's a catch to this. Most if not all NISQ devices can only entangle qubits that are physically close in the device (i.e. neighbouring qubits on 2-d layout in Figure 2.3(14-qubit backend: IBM Q team, "ibmq_16_melbourne v1.0.0" (2019))). Retrieved from https://quantum-computing.ibm.com)). Even if the connectivity is not all-to-all, there's a way to swap qubits states around and entangle any pair in the system. For example from Figure 2.3, if we want to entangle or apply C-Not gate to

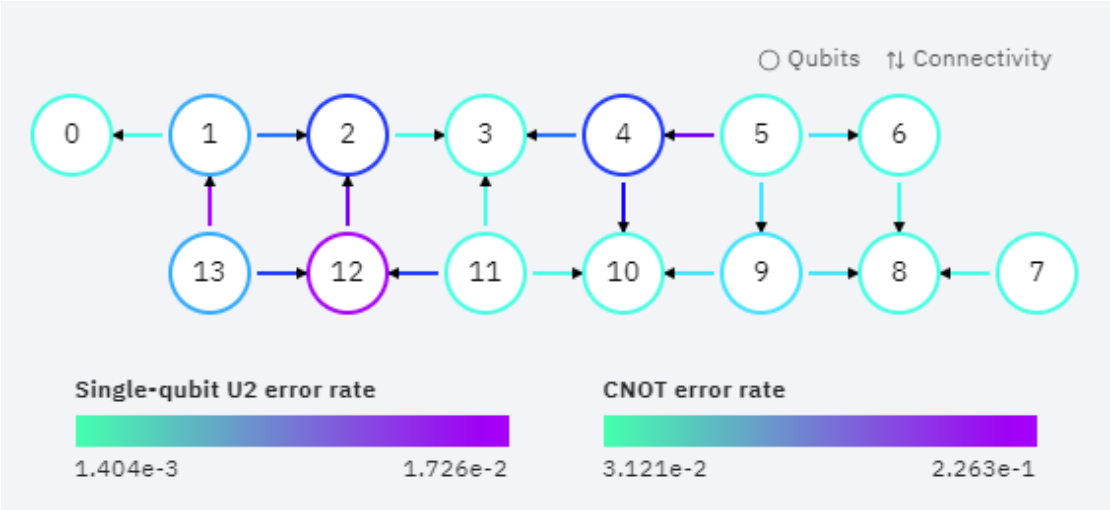


Figure 2.3: Physical connectivity of ibmq_16_melbourne

qubit 8 and 3, we can swap 9 with 8, swap 5 with 9, swap 4 with 5, then apply C-Not from 4 to 3. However naively swapping qubits around will increase circuit depth and increase error to the computation. Smart mapping of which physical qubits needs to be map to our logical qubit in our algorithm is crucial. There are research on making a compiler to help with this problem which is studied in (Zhang et al., 2019).

2.3 Error Mitigation and Correction

Current NISQ devices are not capable of running long and complex algorithms such as Shor's factoring algorithm or Grover's search just yet because these types of algorithm needs exact precision during its computation. Instead of waiting only for qubits properties to improve, there is another field which studies how to use quantum computers with these imperfect qubits. Error correcting and mitigation schemes are proposed such that once the qubit error rate drops below a certain threshold and more qubits are available on the devices, these error correcting method can be used to carry out error-free calculation. Another perspective was proposed recently (Peruzzo et al., 2014; Farhi et al., 2014; Bravo-Prieto et al., 2019; McClean et al., 2016), instead of fighting against noises, algorithms should be designed to be noise robust.

Error Correction Schemes

Error correction on quantum computer can be done with qubit encoding (Roffe, 2019; Gottesman, 2010; Devitt et al., 2013). Example of qubit encodings are bit flip code, sign flip code, Shor code (Shor, 1995), and bosonic code (Cochrane et al., 1999). The most notable encoding is the surface code (Kitaev, 2003; Dennis et al., 2002; Fowler et al., 2012) by which is mimic topological qubits which is fault-tolerant by nature.

Error Mitigation Schemes

Some types of noises such as read out errors or measurement errors can be mitigated easily if devices properties are available. By preparing sets of known quantum states and perform a series of finite measurement on them and recreating Positive-Operator Valued Measure (POVM), classical noise which is the dominant noise in read out error can be mitigated [(Maciejewski et al., 2019; Temme et al., 2017; Kandala et al., 2018)

Noise Robust Algorithm

Recently noise robust algorithms that can be run on NISQ devices are proposed. The two most popular algorithms are Variational Quantum Eigensolver (VQE) (Peruzzo et al., 2014) and Quantum Approximate Optimization Algorithm (QAOA) (Farhi et al., 2014) which requires both quantum computer or quantum processing unit (QPU) and classical computers or classical processing unit (CPU) to work together. VQE and QAOA first initialise some shallow depth circuit, usually refers to as entangler, which entangle qubits with tunable parameters which upon measurement should give high probability of observing good candidate solution to optimisation problems. After observing the result from QPU, classical optimiser is run on CPU to fine tune the entangler parameter and then redo the algorithm on QPU until best answer is found. This type of algorithm is very similar to how evolutionary algorithm or machine learning do things classically.

2.4 Quality Metric of Quantum Circuit

Quantum algorithm, in the early days were mostly inspired by classical algorithm. Since quantum computation needs to be reversible, research on designing quantum circuits took reversible classical computation as based (Gupta et al., 2006; Shende et al., 2003; Maslov and Dueck, 2004; Yang et al., 2008; Prasad et al., 2006; Smolin and DiVincenzo, 1996). The problems they addressed were optimisations of number of garbage bits and quantum cost. Later on, in addition to quantum cost and garbage bits, researchers added number of ancilla qubits, delay (or recently called circuit depth), and the exact synthesis of circuit using some sets of elementary quantum gates (Große et al., 2008; Hung et al., 2006). Around the time when small-scaled quantum computers were realised, multiple cost metrics were discussed in (Maslov and Miller, 2007) and later literature started using new cost metrics such as ancilla count, gate count in terms of elementary gate sets defined by each device, or costly gates with respect to some real devices.

Some commonly used quality metrics or cost metrics in recent literature are briefly described below.

Ancilla Bit Count

Ancilla qubits are extra qubits which is used during computation in addition to input and output qubits to speed up the computation process by reducing total gates or circuit depth (Morimae et al., 2017, 2014). Many works proposed ways to reduce ancilla qubits by increasing circuit depth linear to the number of inputs (Wille et al., 2010). Since most current NISQ devices don't have fully-connected qubits or large number of qubits available, a trade-off between number of ancilla and circuit depth needs to be considered.

Fidelity

Fidelity is a single value describing how close a quantum system is to the ideal system. In this case fidelity may refer to how close the states after computation are to the ideal final states, finding this type of fidelity is done via a method called quantum state tomography (Schmied, 2016; Torlai et al., 2018). Another type of tomography, the quantum process tomography, can be used to find fidelity value of how good circuits are as opposed to the matrix it represents (O'Brien et al., 2004; Knee et al., 2018). Fidelity is usually used to measure the quality of a quantum computer (Wright et al., 2019; Linke et al., 2017; Ballance et al., 2016), how well it can carry out the computation (usually done by randomised benchmarking) (Hashagen et al., 2018; Magesan et al., 2012, 2011), and how close it is to a perfect device. Fidelity is device specific and thus is not used to measure how well a quantum circuit implementation is across different devices.

Circuit Depth

Multiple operations that act upon different independent set of qubits can be done at the same time in most devices. Similar to counting clock cycle in classical circuit design, circuit depth defines the actual time needed for certain circuit to run. Literature focusing on the classical reversible circuits and early works on designing quantum circuit may refer to this as quantum delay. With current NISQ devices, where qubits lifetime is ephemeral, circuit depth is a common metric to consider in most literature.

T-depth and T-count

Clifford gates and T gate is one of the universal gate set in quantum computation (Kliuchnikov et al., 2013). Performing T gate exactly or even within small error threshold is a problem for some kind of quantum computers (Amy et al., 2013) and using T-depth as a cost function was proposed. Many algorithms to optimise circuits to reduce T-depth and T-count was proposed (Amy, 2013; Glaudell et al., 2019;

Selinger, 2014, 2013; Thapliyal and Ranganathan, 2013; Thapliyal et al., 2018; Ross and Selinger, 2016)

C-Not count

For most technologies including superconducting quantum computers, C-Not gate is the most costly gate which requires a longer time and is more error prone than every other basis gates available with respect to its architecture. Most literature, use this metric as a means to compare good circuit design. C-Not optimising algorithms for Linear Nearest Neighbour qubits were proposed in (Cheung et al., 2007; Hirata et al., 2009) and for any quantum computers in general (Nam et al., 2018; Meuli et al., 2018; Muñoz-Coreas and Thapliyal, 2018; Cheng et al., 2015)

Quantum Cost

First proposed in the work of Barenco et al (Barenco et al., 1995) as a metric for designing efficient quantum computations using elementary gate set. It is defined as the total gate count of arbitrary single qubit gate and arbitrary two-qubit gate. Multiple variants of this quantum cost were proposed after prototypes of quantum computers were realisable, such as in the work of (Vedral et al., 1996). Circuit optimisation algorithms were proposed to reduce this cost (Hung et al., 2006; Lukac et al., 2017)

Qiskit Cost

Proposed by IBM to be used as a cost for circuits running on IBM QX devices (Zhang et al., 2019). This cost function was used by multiple competitions from IBM Q to find efficient quantum circuit compiler and designing efficient quantum algorithms. The cost is defined by 10m + n where m is the number of C-Not gate and n is the number of single qubit gate. The idea behind this cost function came from characteristics of IBM QX devices and superconducting quantum computers from other providers (Arute et al., 2019; Reagor et al., 2018) that C-Not gate or

basis two-qubit gate has around 10 times error rate of that single qubit gate.

Chapter III

REVIEW OF LITERATURE

Binary arithmetic are core components to classical computing. Similarly to quantum computers, in the early days people tried to mimic this approach of building circuits from building blocks such as adder, comparator, and multiplier circuit. Since Shor's algorithm for factoring and discrete logarithm was proposed. Newer approach to arithmetic via quantum means such as teleportation based operations (Van Meter et al., 2008), measurement based schemes on cluster states (Trisetyarso and Van Meter, 2010), or repeat-until-success circuits (Wiebe and Roetteler, 2016). Taken after Shor's Quantum Fourier Transform approach, multiple QFT adders and multipliers were proposed (Beauregard, 2003; Beauregard et al., 2003; Pavlidis and Gizopoulos, 2014; Maynard and Pius, 2014). Even looking further into the future, multi-computer arithmetic operations were studied in (Van Meter et al., 2008; Jones et al., 2012).

In the next following subsection, various approaches into building quantum adder and quantum comparator will be discussed in brief details.

3.1 Adder inspired by classical reversible circuit

Based on classical reversible circuits, this type of quantum adder encode the number to be added using binary representation (or base-d number for d-level quantum systems). One of the first designs were proposed by Vedral, Barenco and Ekert in 1996 (Vedral et al., 1996). Vedral adder was then later improved by multiple works (Gossett, 1998; Cheng and Tseng, 2002; Chakrabarti and Sur-Kolay, 2008) but the most notable one is from Cuccaro in which ripple carry adder was proposed (Cuccaro et al., 2004). Vedral adder also used as a based for floating point adder (Nachtigal et al., 2011; Nguyen and Van Meter, 2014), Binary Coded Deci-

mal adder (Nagamani et al., 2014), adder for sets of numbers stored in superposition states (Lu et al., 2018), approximate adder (Alvarez-Rodriguez et al., 2015), probabilistic adder (Lau et al., 2010), and the realisation of adder on ion-trapped device (Barbosa, 2006).

An improved version of Cuccaro adder was proposed in (Wang et al., 2016) which reduces the work of cleanup intermediate value by reorder input states. Cuccaro adder also got many applications to it. Some examples of the applications are approximate adder specialised for Shor's algorithm (Gidney, 2019; Zalka, 2006), optimal T-depth division circuit (Thapliyal et al., 2018), optimal R gate adder (Montaser et al., 2019), and devising algorithms for linear nearest neighbour quantum computers (Hirata et al., 2009; Choi and Van Rodney, 2011; Choi and Meter, 2012).

3.2 Adder using Quantum Fourier Transform

Began with Shor's factoring algorithm, the factoring algorithm requires a process to solve it namely; after computing $f(x)$ then compute $f(x+y)$. Where $f(x)$ takes x into the transform space by QFT. Inspired by Shor's adder and in the hope of speeding up factoring algorithm, one of the first few notable improvements on QFT adder on this was done by Draper (Draper, 2000). Draper's QFT adder was then later optimised by many researchers (Gidney, 2018, 2017; Florio and Picca, 2004) and were used as a base for quantum modular exponential (Pavlidis and Gizopoulos, 2014; Amy et al., 2013), floating point adder (Thapliyal and Ranganathan, 2013), quantum hybrid multiplier (Maynard and Pius, 2013), and mean finding algorithm and weight sum algorithm (Ruiz-Perez and Garcia-Escartin, 2017). Variants from Draper's QFT adder also got applications for QFT-based algorithm and improved version of Shor's algorithm (Asaka et al., 2019; Beauregard, 2003) and also the realisation of QFT adder on multiple experimental setup (Choi and Meter, 2012).

3.3 Quantum Comparator

Realising quantum comparator circuit can be done via two means.

First approach is to use quantum adder. When comparing two binary numbers A and B, if one wants to check whether A is larger than B, by complementing B into B'. By adding A and B' together, checking the carry output bit, it can tell us whether A is larger than B or not. This first approach does not need specialised circuits and can be done by a little modification on quantum adder and reverse the add procedure to clean ancilla bit. Analysis on this modification can be seen in (Cuccaro et al., 2004; Vedral et al., 1996) for plain quantum adder and (Draper, 2000; Gidney, 2017) for QFT adder.

Second approach to building quantum comparator is to directly design sub circuit to compare each bit of the number similar to classical ripple comparator approach. Most literature on this approach were done with the aim of optimising quantum cost (Beckman et al., 1996; Sarker et al., 2014; Oliveira et al., 2006). No literature on this approach which focus on optimising C-Not can be found.

3.4 Multiple Controlled Toffoli Gate

One basic component in classical when doing arithmetic and Boolean algebra is the "and" operation. Reversible "AND" operation is usually done via multiple controlled-Toffoli gate (MCT) in quantum computing and since "AND" is a very basic operation. Works on classical reversible circuit which tend to optimise quantum cost usually use lots of MCT with both positive and negative controls and Peres gate (which is also a variant of MCT). Optimising MCT can help the circuit in general to achieve better quantum cost and reduction on C-Not gate count. Multiple techniques on finding better designs of MCT such as computer aided design (Nam et al., 2018), linear depth MCT with no ancilla but assuming arbitrary two qubit control gate (Saeedi and Pedram, 2013), single T-depth MCT design (Selinger, 2013),

using relative phase version of operations with ancilla bits which later got reversed reducing both T-count and C-not count (Maslov, 2016).

Chapter IV

PROPOSED CIRCUIT

In this chapter we study in detail how to optimise the implementations of the quantum comparator circuit, show how we extend circuits from literature to achieve this new circuit.

From Cuccaro's quantum adder, core part of it is the MAJ circuit (or gate). MAJ gate accepts three qubits input and also output three qubits. Operation of MAJ gate is to find the *majority* of the input and permute it in such a way that the majority (of either 0 or 1) will be output in the lowest line of qubit (see Figure 4.1 for the circuit model).

To build quantum comparator that outputs whether A is more than B or not. We took Cuccaro adder and modified it using the extension in (Cuccaro et al., 2004). Since we only interest in the highest bit of the adder and we don't care about the sum result. We can build quantum comparator by propagating the carry (or the majority of three qubit) to the most significant bit, put it in the output bit, and reverse the majority step. Figure 4.2 depicts three bit quantum comparator using this method, output bit at s_0.

Taking controlled-Not gate optimisation method from (Maslov, 2016), we can use the same techniques of using relative phase to make relative phase MAJ gate (RMAJ) gate. One version of relative phase Toffoli gate, Margolous gate, is

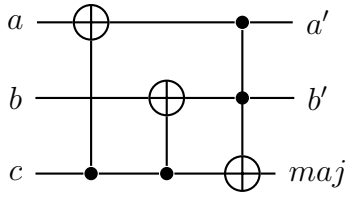


Figure 4.1: majority gate (MAJ)

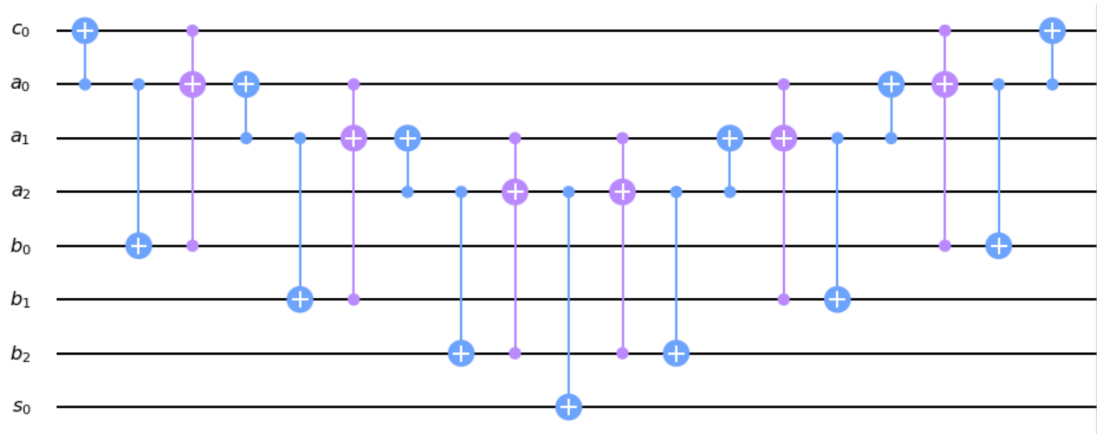


Figure 4.2: quantum comparator based on Cuccaro adder

depicted in Figure 4.3. By replacing Toffoli gate in MAJ gate with Margolous gate, this RMAJ gate will only differ to MAJ on $|011\rangle$ input, which maps $|011\rangle$ to $-|101\rangle$ instead of $|101\rangle$. This phase difference does not pose a problem since our entire circuit does not rely on phase change during the carry ripple process. Also we fix the phase back to its original phase using inverse of RMAJ (iRMAJ) which can be implemented easily by reversing gate order and inverting the gate.

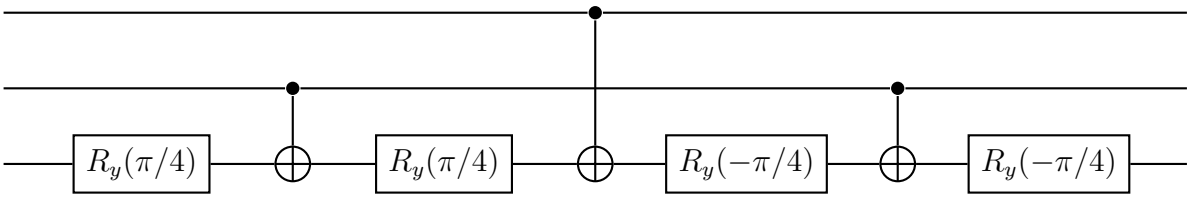


Figure 4.3: Margolous gate

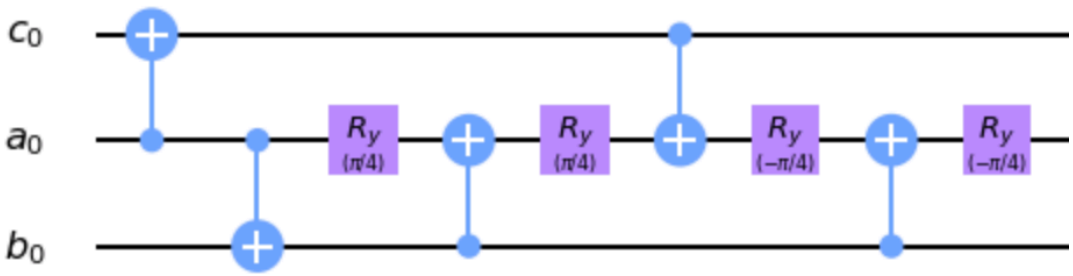


Figure 4.4: reverse majority gate (RMAJ)

Algorithm 1: greater than

input : $A = a_{n-1}a_{n-2}a_{n-3}\ldots a_0$, $B = b_{n-1}b_{n-2}b_{n-3}\ldots b_0$, $z = z$, $c = 0$

output: $A = a_{n-1}a_{n-2}a_{n-3}\ldots a_0$, $B = b_{n-1}b_{n-2}b_{n-3}\ldots b_0$, $z = z \oplus s_n$, $c = 0$

for $i \leftarrow 0$ **to** $n-1$ **do**

  $b_i \leftarrow\sim b_i$

$b_0 \leftarrow MAJ(a_0, b_0, c)$

for $i \leftarrow 1$ **to** $n-1$ **do**

  $b_i \leftarrow MAJ(a_i, b_i, b_{i-1})$

$z \leftarrow z \oplus b_{n-1}$

for $i \leftarrow n-1$ **to** 1 **do**

  $b_i \leftarrow RMAJ(a_i, b_i, b_{i-1})$

$b_0 \leftarrow RMAJ(a_0, b_0, c)$

for $i \leftarrow 0$ **to** $n-1$ **do**

  $b_i \leftarrow\sim b_i$

Chapter V

RESULTS

In this chapter, we will summarise our proposed quantum comparator circuit to Cuccaro's comparator, VBE comparator, and ripple carry comparator generalised from (Sarker et al., 2014; Oliveira et al., 2006; Beckman et al., 1996). The result we compared were not from their original papers but rather their implementation on superconducting IBM QX device. All candidate comparator circuits were transpiled from circuit model into IBM QX device native gates of arbitrary single qubit and C-Not gate. We also report the 2-qubit comparator running on IBM QX devices.

The reason we do not include QFT based adder in our comparison is due to the fact that depth defined on all QFT based adder literature assumed arbitrary two-qubit gate as having depth one. Implementing QFT based circuit using C-Not as only two qubit gate would increase too much depth and we do not see any reason to compare circuits that were optimised based on different assumptions and goals.

We tested our proposed 2-bit quantum comparator circuit with Grover's

Adder	Number of bits	Number of anc. bits	C-Not count	Qiskit cost
Proposed circuit	$2n$	1	$10n+1$	$108n+10$
VBE	$2n$	n	$28n-14$	$312n-156$
Cuccaro	$2n$	1	$16n-5$	$176n+10$
Ripple Comparator	$2n$	n	$O(n^2)$	$O(n^2)$

Table 5.1: Circuit cost summary for $n \geq 3$. We then listed number of input bits, number of ancilla bits, C-Not count, and Qiskit cost. We do not include the complementing step but only the high bit finding part.

algorithm by setting search threshold to be 2. We do one Grover iteration for the comparison step which in the ideal scenario, should output 00011 with 100% of the time. We tested the same circuit on three devices; ibmq_vigo, ibmq_ourense and ibmqx2 (5-qubit backend: IBM Q team, "ibmqx2 v2.0.1", "ibmq_vigo v1.0.2", "ibmq_ourense v1.0.1", (2019). Retrieved from https://quantum-computing.ibm.com) with 8196 shots per device. As we can see slightly in computation result, it seems to have a correlated output 00001 and 00011 higher than the rest. Our assumptions on the outcome is that since the fourth output bit of all devices has short decoherence time (both T1 and T2) the 1 in the fourth bit might lose its 1 component before computation ends.

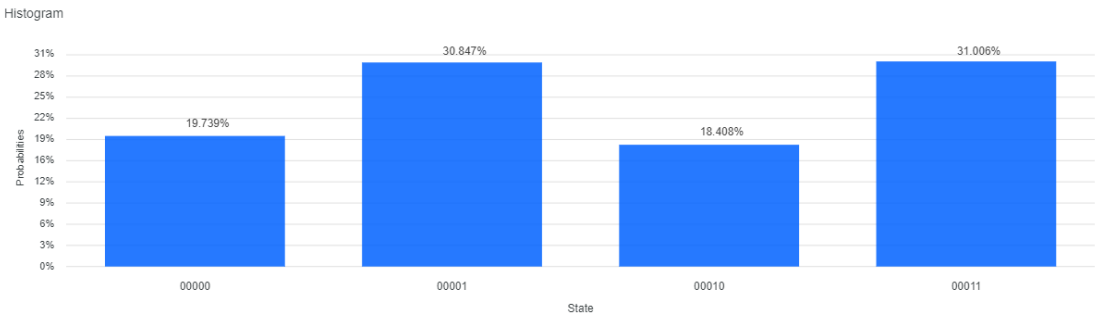


Figure 5.1: Proposed circuit result from ibmq_vigo

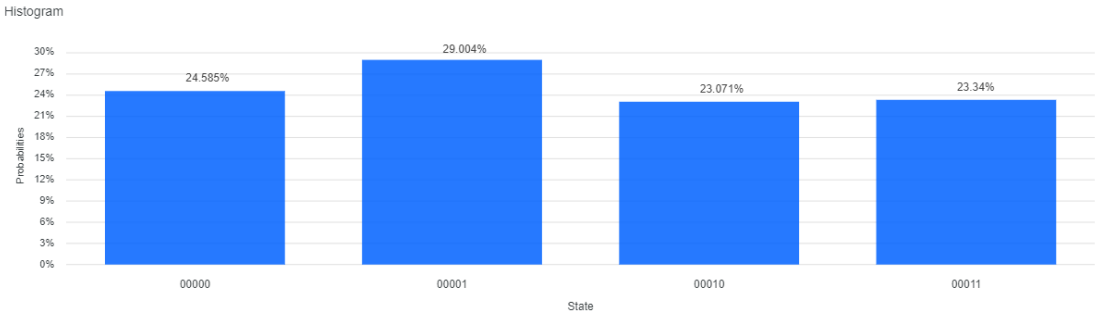


Figure 5.2: Proposed circuit result from ibmq_ourense

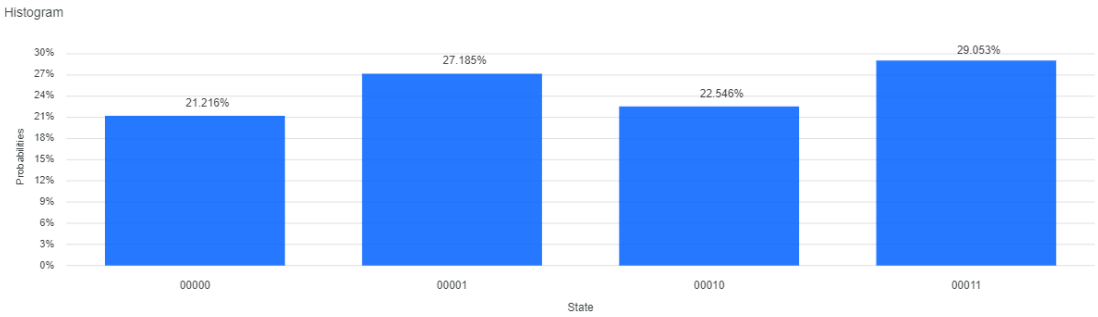


Figure 5.3: Proposed circuit result from ibmqx2

Chapter VI

DISCUSSION

6.1 Summary of Findings

From the results of comparing our proposed circuits with other quantum comparator circuit from literature, we can see that using Maslov's relative phase optimising techniques is a promising approach to optimise circuit cost defined by C-Not count and Qiskit cost. Comparator circuit is a very small compare to most problem specific oracle circuits. We can see a huge improvement on C-Not count and Qiskit cost even from optimising comparator circuit which suggests that if we use the same techniques on larger and more complex circuit, its cost should be reduced with higher efficiency.

Another perspective to the results is that as we know more device properties, in this case its native elementary gate. Given the correct cost factor with respected to each device to minimise, every circuit should be able to become smaller and much more efficient.

For the real device results, we can see strong signs that output has some correlation with the ideal output states with only the fourth qubit high error rate. We expect that by using error read out mitigation scheme, we might be able to see better results. With the three devices we tested on, it seems that shallow depth circuit might be able incorporate our proposed quantum circuit while still not losing all the quantum properties of the qubit after computation ends.

It is important to note that our scope of optimisation in this thesis is to reduce C-Not count and Qiskit cost, but another significant factor one should consider when running on real device is circuit depth. As can be seen from Table 5.1, one might wonder why ripple comparator cost is in $O(n^2)$, it is due to the fact that parts of

ripple comparator can be perform in parallel. Parallel or multi-quantum computer given large enough input might have lower circuit depth and circuit cost for each quantum computer.

6.2 Future Work

Maslov's technique of turning parts of circuit into relative phase variant and later readjust the phase back is only one technique to be used. There still are many parts available to be optimised, such as combining two RMAJ gate to permute states of five inputs instead of three at a time. Another interesting circuit to optimise is the adder circuit since it is a very important subroutine which is used by many algorithms such as Shor's factoring and some oracles of optimisation problems. A good candidate for base adder is from (Wang et al., 2016), which can also be used with the same relative phase techniques.

6.3 Open Problems

As suggested in (Maslov, 2016), it is hard to systematically synthesise relative phase version of circuits. Computer-aided Design (CAD), evolutionary algorithm, or machine learning algorithm might be able to help us find better circuits. A new cost function might need to be considered to better suit newer devices since there is progress on adding more native elementary two-qubit gate to superconducting device Abrams et al. (2019). There might even be a better scheme than relative phase version to optimise as there might be a connection between balancing circuit cost and ancilla count and it will be much more important for devices with larger qubits in the near future.

REFERENCES

Aaronson, S. 2010. BQP and the polynomial hierarchy. In Proceedings of the Annual ACM Symposium on Theory of Computing, pp. 141–150. :

Aaronson, S. 2013. Quantum Computing since Democritus. Cambridge University Press. doi: 10.1017/cbo9780511979309.

Aaronson, S. 2014. Quantum Machine Learning Algorithms: Read the Fine Print. Technical report.

Aaronson, S. and Ambainis, A. 2014. The need for structure in quantum speedups. Theory of Computing 10 (aug 2014): 133–166.

Aaronson, S. and Chen, L. 2017. Complexity-theoretic foundations of quantum supremacy experiments. Technical report.

Abrams, D. M., Didier, N., Johnson, B. R., da Silva, M. P., and Ryan, C. A. 2019. Implementation of the XY interaction family with calibration of a single pulse. (dec 2019):

Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Lütkenhaus, N., Monyk, C., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H., and Zeilinger, A. 2014. Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science 560.P1 (2014): 62–81.

Alvarez-Rodriguez, U., Sanz, M., Lamata, L., and Solano, E. 2015. The Forbidden Quantum Adder. Technical report.

Amy, M. 2013. Algorithms for the Optimization of Quantum Circuits. Technical report.

Amy, M., Maslov, D., Mosca, M., and Roetteler, M. 2013. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits.

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 32.6 (jun 2013): 818–830.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., Fowler, A., Gidney, C., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M. P., Hartmann, M. J., Ho, A., Hoffmann, M., Huang, T., Humble, T. S., Isakov, S. V., Jeffrey, E., Jiang, Z., Kafri, D., Kechedzhi, K., Kelly, J., Klimov, P. V., Knysh, S., Korotkov, A., Kostritsa, F., Landhuis, D., Lindmark, M., Lucero, E., Lyakh, D., Mandrà, S., McClean, J. R., McEwen, M., Megrant, A., Mi, X., Michielsen, K., Mohseni, M., Mutus, J., Naaman, O., Neeley, M., Neill, C., Niu, M. Y., Ostby, E., Petukhov, A., Platt, J. C., Quintana, C., Rieffel, E. G., Roushan, P., Rubin, N. C., Sank, D., Satzinger, K. J., Smelyanskiy, V., Sung, K. J., Trevithick, M. D., Vainsencher, A., Villalonga, B., White, T., Yao, Z. J., Yeh, P., Zalcman, A., Neven, H., and Martinis, J. M. 2019. Quantum supremacy using a programmable superconducting processor. Nature 574.7779 (oct 2019): 505–510.

Asaka, R., Sakai, K., and Yahagi, R. 2019. Quantum Circuit for the Fast Fourier Transform. (nov 2019):

Ballance, C. J., Harty, T. P., Linke, N. M., Sepiol, M. A., and Lucas, D. M. 2016. High-Fidelity Quantum Logic Gates Using Trapped-Ion Hyperfine Qubits. Physical Review Letters 117.6 (dec 2016):

Barbosa, G. A. 2006. Quantum half-adder. Physical Review A - Atomic, Molecular, and Optical Physics 73.5 (2006):

Barenco, A., Bennett, C. H., Cleve, R., Divincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A., and Weinfurter, H. 1995. Elementary gates for quantum computation. Physical Review A 52.5 (mar 1995): 3457–3467.

Beauregard, S. 2003. Circuit for Shor's algorithm using 2n+3 qubits. Technical Report 2.

Beauregard, S., Brassard, G., and Fernandez, J. M. 2003. Quantum Arithmetic on Galois Fields. (jan 2003):

Beckman, D., Chari, A. N., Devabhaktuni, S., and Preskill, J. 1996. Efficient networks for quantum factoring. Technical Report 2.

Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. 1997. Strengths and weaknesses of quantum computing. SIAM Journal on Computing 26.5 (1997): 1510–1523.

Bernstein, E. and Vazirani, U. 1997. Quantum complexity theory. SIAM Journal on Computing 26.5 (oct 1997): 1411–1473.

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., and Lloyd, S. 2017. Quantum machine learning. Technical Report 7671.

Blundo, C., D'Arco, P., Daza, V., and Padró, C. 2004. Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures. Theoretical Computer Science 320.2-3 (jun 2004): 269–291.

Boyer, M., Brassard, G., HØyer, P., and Tapp, A. 1998. Tight bounds on quantum searching. Fortschritte der Physik 46.4-5 (may 1998): 493–505.

Brakerski, Z., Christiano, P., Mahadev, U., Vazirani, U., and Vidick, T. 2018. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS, volume 2018-Octob, pp. 320–331. : IEEE Computer Society.

Brassard, G., Høyer, P., Mosca, M., and Tapp, A. 2002. Quantum amplitude amplification and estimation. Technical report.

Bravo-Prieto, C., LaRose, R., Cerezo, M., Subasi, Y., Cincio, L., and Coles, P. J. 2019. Variational Quantum Linear Solver: A Hybrid Algorithm for Linear Systems. (sep 2019):

Chakrabarti, A. and Sur-Kolay, S. 2008. Designing quantum adder circuits and evaluating their error performance. In 2008 International Conference on Electronic Design, ICED 2008. :

Cheng, C. S., Singh, A. K., and Gopal, L. 2015. Efficient Three Variables Reversible Logic Synthesis Using Mixed-polarity Toffoli Gate. In Procedia Computer Science, volume 70, pp. 362–368. : Elsevier B.V.

Cheng, K.-W. and Tseng, C.-C. 2002. Quantum Plain and Carry Look-Ahead Adders. arXiv:quant-ph/0206028 (jun 2002): 1–16.

Cheung, D., Maslov, D., and Severini, S. 2007. Translation Techniques Between Quantum Circuit Architectures. Workshop on Quantum Information Processing (2007): 1–3.

Choi, B. S. and Meter, R. V. 2012. A Θ(Mathematical Equation Presented)-depth quantum adder on the 2D NTC quantum computer architecture. ACM Journal on Emerging Technologies in Computing Systems 8.3 (aug 2012):

Choi, B. S. and Van Rodney, M. 2011. On the effect of quantum interaction distance on quantum addition circuits. ACM Journal on Emerging Technologies in Computing Systems 7.3 (sep 2011):

Cochrane, P. T., Milburn, G. J., and Munro, W. J. 1999. Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping. Physical Review A - Atomic, Molecular, and Optical Physics 59.4 (sep 1999): 2631–2634.

Cuccaro, S. A., Draper, T. G., Kutin, S. A., and Moulton, D. P. 2004. A new quantum ripple-carry addition circuit. (oct 2004):

Dawson, C. M. and Nielsen, M. A. 2006. The Solovay-Kitaev algorithm. Quantum Information and Computation 6.1 (jan 2006): 081–095.

Dennis, E., Kitaev, A., Landahl, A., and Preskill, J. 2002. Topological quantum memory. Journal of Mathematical Physics 43.9 (oct 2002): 4452–4505.

Deutsch, D. 1985. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer.. Proceedings of The Royal Society of London, Series A: Mathematical and Physical Sciences 400.1818 (jul 1985): 97–117.

Deutsch, D. and Jozsa, R. 1992. Rapid Solution of Problems by Quantum Computation. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 439.1907 (dec 1992): 553–558.

Devitt, S. J., Munro, W. J., and Nemoto, K. 2013. Quantum error correction for beginners. Technical Report 7.

Draper, T. G. 2000. Addition on a Quantum Computer. (aug 2000):

Farhi, E., Goldstone, J., and Gutmann, S. 2014. A Quantum Approximate Optimization Algorithm. (nov 2014):

Feynman, R. P. 1982. Simulating physics with computers. International Journal of Theoretical Physics 21.6-7 (jun 1982): 467–488.

Florio, G. and Picca, D. 2004. Quantum implementation of elementary arithmetic operations. (mar 2004):

Fowler, A. G., Mariantoni, M., Martinis, J. M., and Cleland, A. N. 2012. Surface codes: Towards practical large-scale quantum computation. Physical Review A - Atomic, Molecular, and Optical Physics 86.3 (aug 2012):

Fujii, K., Kobayashi, H., Morimae, T., Nishimura, H., Tamate, S., and Tani, S. 2018. Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error. Technical Report 20.

Gidney, C. 2017. Factoring with n+2 clean qubits and n-1 dirty qubits. (jun 2017):

Gidney, C. 2018. Halving the cost of quantum addition. Quantum 2 (sep 2018): 74.

Gidney, C. 2019. Approximate encoded permutations and piecewise quantum adders. Technical report.

Glaudell, A. N., Ross, N. J., and Taylor, J. M. 2019. Canonical forms for single-qutrit Clifford+T operators. Technical report.

Gossett, P. 1998. Quantum Carry-Save Arithmetic. (aug 1998):

Gottesman, D. 2010. An introduction to quantum error correction and fault-tolerant quantum computation. pp. 13–58. :

Große, D., Wille, R., Dueck, G. W., and Drechsler, R. 2008. Exact synthesis of elementary quantum gate circuits for reversible functions with don't cares. In Proceedings of The International Symposium on Multiple-Valued Logic, pp. 214–219. :

Grover, L. K. 1997. Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters 79.2 (jun 1997): 325–328.

Gupta, P., Agrawal, A., and Jha, N. K. 2006. An algorithm for synthesis of reversible logic circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 25.11 (nov 2006): 2317–2329.

Harrow, A. W. and Montanaro, A. 2017. Quantum computational supremacy. Nature 549.7671 (sep 2017): 203–209.

Harrow, A. W., Hassidim, A., and Lloyd, S. 2009. Quantum algorithm for linear systems of equations. Physical Review Letters 103.15 (nov 2009):

Hashagen, A. K., Flammia, S. T., Gross, D., and Wallman, J. J. 2018. Real Randomized Benchmarking. Quantum 2 (feb 2018): 85.

Hirata, Y., Nakanishi, M., Yamashita, S., and Nakashima, Y. 2009. An efficient method to convert arbitrary quantum circuits to ones on a linear nearest

neighbor architecture. In Proceedings of the 3rd International Conference on Quantum, Nano and Micro Technologies, ICQNM 2009, pp. 26–33. :

Hor-Meyll, M., Tasca, D. S., Walborn, S. P., Ribeiro, P. H., Santos, M. M., and Duzzioni, E. I. 2015. Deterministic quantum computation with one photonic qubit. Technical Report 1.

Hung, W. N., Song, X., Yang, G., Yang, J., and Perkowski, M. 2006. Optimal synthesis of multiple output Boolean functions using a set of quantum gates by symbolic reachability analysis. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 25.9 (sep 2006): 1652–1663.

Ithier, G., Collin, E., Joyez, P., Meeson, P. J., Vion, D., Esteve, D., Chiarello, F., Shnirman, A., Makhlin, Y., Schriefl, J., and Schön, G. 2005. Decoherence in a superconducting quantum bit circuit. Physical Review B - Condensed Matter and Materials Physics 72.13 (aug 2005):

Jones, J. A. 2001. Quantum computing and nuclear magnetic resonance [Online]. Available from: http://xlink.rsc.org/?DOI=b103231n [2001,jan].

Jones, N. C., Van Meter, R., Fowler, A. G., McMahon, P. L., Kim, J., Ladd, T. D., and Yamamoto, Y. 2012. Layered architecture for quantum computing. Technical Report 3.

Kandala, A., Temme, K., Corcoles, A. D., Mezzacapo, A., Chow, J. M., and Gambetta, J. M. 2018. Extending the computational reach of a noisy superconducting quantum processor. Technical report.

Kerenidis, I. and Prakash, A. 2017. Quantum recommendation system. In Leibniz International Proceedings in Informatics, LIPIcs, volume 67. : Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing.

Kitaev, A. Y. 1995. Quantum measurements and the Abelian Stabilizer Problem. (nov 1995):

Kitaev, A. Y. 2003. Fault-tolerant quantum computation by anyons. Annals of Physics 303.1 (jul 2003): 2–30.

Kliuchnikov, V., Maslov, D., and Mosca, M. 2013. Fast and efficient exact synthesis of single-qubit unitaries generated by clifford and T gates. Technical Report 7-8.

Knee, G. C., Bolduc, E., Leach, J., and Gauger, E. M. 2018. Quantum process tomography via completely positive and trace-preserving projection. Physical Review A 98.6 (mar 2018):

Knill, E. and Laflamme, R. 1998. Power of one bit of quantum information. Physical Review Letters 81.25 (1998): 5672–5675.

Koller, J., Bender, W., and Barabasi, I. 2019. Exploring Quantum Approximations of Traveling Salesman. Technical report.

Lau, M. S., Ling, K. V., Chu, Y. C., and Bhanu, A. 2010. Modeling of probabilistic ripple-carry adders. In Proceedings - 5th IEEE International Symposium on Electronic Design, Test and Applications, DELTA 2010, pp. 201–206. :

Linke, N. M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K. A., Wright, K., and Monroe, C. 2017. Experimental comparison of two quantum computing architectures. Technical Report 13.

Lu, X., Jiang, N., Hu, H., and Ji, Z. 2018. Quantum Adder for Superposition States. International Journal of Theoretical Physics 57.9 (sep 2018): 2575–2584.

Lukac, M., Kameyama, M., Perkowski, M., and Kerntopf, P. 2017. Minimization of Quantum Circuits using Quantum Operator Forms. (jan 2017):

Maciejewski, F. B., Zimborás, Z., and Oszmaniec, M. 2019. Mitigation of readout noise in near-term quantum devices by classical post-processing based on detector tomography. (jul 2019):

Magesan, E., Gambetta, J. M., and Emerson, J. 2011. Scalable and robust randomized benchmarking of quantum processes. Physical Review Letters 106.18 (sep 2011):

Magesan, E., Gambetta, J. M., and Emerson, J. 2012. Characterizing quantum gates via randomized benchmarking. Physical Review A - Atomic, Molecular, and Optical Physics 85.4 (apr 2012):

Maslov, D. 2016. Advantages of using relative-phase Toffoli gates with an application to multiple control Toffoli optimization. Physical Review A 93.2 (2016):

Maslov, D. and Dueck, G. W. 2004. Reversible cascades with minimal garbage. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 23.11 (nov 2004): 1497–1509.

Maslov, D. and Miller, D. M. 2007. Comparison of the Cost Metrics for Reversible and Quantum Logic Synthesis. IET Computers & Digital Techniques, 1(2) (nov 2007): 98–104.

Maynard, C. M. and Pius, E. 2013. Integer Arithmetic With Hybrid Quantum-Classical Circuits. (apr 2013):

Maynard, C. M. and Pius, E. 2014. A quantum multiply-accumulator. Quantum Information Processing 13.5 (2014): 1127–1138.

McClean, J. R., Romero, J., Babbush, R., and Aspuru-Guzik, A. 2016. The theory of variational hybrid quantum-classical algorithms. New Journal of Physics 18.2 (sep 2016):

Meuli, G., Soeken, M., and De Micheli, G. 2018. SAT-based {CNOT, T} quantum circuit synthesis. Technical report.

Mitarai, K., Negoro, M., Kitagawa, M., and Fujii, K. 2018. Quantum circuit learning. Technical Report 3.

Montanaro, A. 2016. Quantum algorithms: An overview. npj Quantum Information 2.1 (nov 2016):

Montaser, R., Younes, A., and Abdel-Aty, M. 2019. New Design of Reversible Full Adder/Subtractor Using R Gate. International Journal of Theoretical Physics 58.1 (aug 2019): 167–183.

Morimae, T., Fujii, K., and Fitzsimons, J. F. 2014. Hardness of classically simulating the one-clean-qubit model. Technical Report 13.

Morimae, T., Fujii, K., and Nishimura, H. 2017. Power of one nonclean qubit. Physical Review A 95.4 (oct 2017):

Muñoz-Coreas, E. and Thapliyal, H. 2018. T-count and qubit optimized quantum circuit design of the non-restoring square root algorithm. Technical Report 3.

Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M. D., and Jiang, L. 2016. Optimal architectures for long distance quantum communication. Scientific Reports 6 (sep 2016):

Myers, J. M., Fahmy, A. F., Glaser, S. J., and Marx, R. 2001. Rapid solution of problems by nuclear-magnetic-resonance quantum computation. Physical Review A - Atomic, Molecular, and Optical Physics 63.3 (2001): 1–8.

Nachtigal, M., Thapliyal, H., and Ranganathan, N. 2011. Design of a reversible floating-point adder architecture. ISBN 9781457715143. doi: 10.1109/NANO.2011.6144358.

Nagamani, A. N., Ashwin, S., and Agrawal, V. K. 2014. Design of optimized reversible binary adder/subtractor and BCD adder. In Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014, pp. 774–779. :

Nam, Y., Ross, N. J., Su, Y., Childs, A. M., and Maslov, D. 2018. Automated optimization of large quantum circuits with continuous parameters. Technical

Report 1.

Nguyen, T. D. and Van Meter, R. 2014. A resource-efficient design for a reversible floating point adder in quantum computing. ACM Journal on Emerging Technologies in Computing Systems 11.2 (jun 2014):

Nielsen, M. A. and Chuang, I. L. 2010. Quantum Computation and Quantum Information. doi: 10.1017/cbo9780511976667.

O'Brien, J. L., Pryde, G. J., Gilchrist, A., James, D. F., Langford, N. K., Ralph, T. C., and White, A. G. 2004. Quantum process tomography of a controlled-NOT gate. Technical Report 8.

Oliveira, D. S., De Sousa, P. B. M., and Ramos, R. V. 2006. Quantum search algorithm using quantum bit string comparator. In 2006 International Telecommunications Symposium, ITS, pp. 582–585. : IEEE.

Pavlidis, A. and Gizopoulos, D. 2014. Fast quantum modular exponentiation architecture for shor's factoring algorithm. Technical Report 7-8.

Peruzzo, A., McClean, J., Shadbolt, P., Yung, M. H., Zhou, X. Q., Love, P. J., Aspuru-Guzik, A., and O'Brien, J. L. 2014. A variational eigenvalue solver on a photonic quantum processor. Nature Communications 5 (apr 2014):

Prasad, A. K., Shende, V. V., Markov, I. L., Hayes, J. P., and Patel, K. N. 2006. Data structures and algorithms for simplifying reversible circuits. ACM Journal on Emerging Technologies in Computing Systems 2.4 (oct 2006): 277–293.

Preskill, J. 2012. Quantum computing and the entanglement frontier. (mar 2012):

Preskill, J. 2018. Quantum Computing in the NISQ era and beyond. Quantum 2 (jan 2018): 79.

Qiang, X., Zhou, X., Wang, J. J. B., Wilkes, C. M., Loke, T., O'gara, S., Kling, L., Marshall, G. D., Santagati, R., Ralph, T. C., Wang, J. J. B., O'brien,

J. L., Thompson, M. G., Matthews, J. C. F., O'Gara, S., Kling, L., Marshall, G. D., Santagati, R., Ralph, T. C., Wang, J. J. B., O'Brien, J. L., Thompson, M. G., and Matthews, J. C. F. 2018. Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. Nature Photonics 12.9 (sep 2018): 534–539.

Reagor, M., Osborn, C. B., Tezak, N., Staley, A., Prawiroatmodjo, G., Scheer, M., Alidoust, N., Sete, E. A., Didier, N., Da Silva, M. P., Acala, E., Angeles, J., Bestwick, A., Block, M., Bloom, B., Bradley, A., Bui, C., Caldwell, S., Capelluto, L., Chilcott, R., Cordova, J., Crossman, G., Curtis, M., Deshpande, S., El Bouayadi, T., Girshovich, D., Hong, S., Hudson, A., Karalekas, P., Kuang, K., Lenihan, M., Manenti, R., Manning, T., Marshall, J., Mohan, Y., O'Brien, W., Otterbach, J., Papageorge, A., Paquette, J. P., Pelstring, M., Polloreno, A., Rawat, V., Ryan, C. A., Renzas, R., Rubin, N., Russel, D., Rust, M., Scarabelli, D., Selvanayagam, M., Sinclair, R., Smith, R., Suska, M., To, T. W., Vahidpour, M., Vodrahalli, N., Whyland, T., Yadav, K., Zeng, W., and Rigetti, C. T. 2018. Demonstration of universal parametric entangling gates on a multi-qubit lattice. Technical Report 2.

Roffe, J. 2019. Quantum error correction: an introductory guide. Technical report.

Ross, N. J. and Selinger, P. 2016. Optimal ancilla-free clifford+T approximation of Z-rotations. Technical Report 11-12.

Ruiz-Perez, L. and Garcia-Escartin, J. C. 2017. Quantum arithmetic with the quantum Fourier transform. Quantum Information Processing 16.6 (nov 2017):

Saeedi, M. and Pedram, M. 2013. Linear-depth quantum circuits for n-qubit Toffoli gates with no ancilla. Physical Review A - Atomic, Molecular, and Optical Physics 87.6 (mar 2013):

Sarker, A., Amin, M. S., Bose, A., and Islam, N. 2014. An optimized design of binary comparator circuit in quantum computing. In 2014 International Conference on Informatics, Electronics and Vision, ICIEV 2014, pp. 1–5.

:

Schmied, R. 2016. Quantum state tomography of a single qubit: comparison of methods. Journal of Modern Optics 63.18 (jul 2016): 1744–1758.

Selinger, P. 2013. Quantum circuits of T-depth one. Physical Review A - Atomic, Molecular, and Optical Physics 87.4 (oct 2013):

Selinger, P. 2014. Efficient Clifford+T approximation of single-qubit operators. Technical Report 1-2.

Shende, V. V., Prasad, A. K., Markov, I. L., and Hayes, J. P. 2003. Synthesis of reversible logic circuits. In IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, volume 22, pp. 710–722. :

Shor, P. W. 1995. Scheme for reducing decoherence in quantum computer memory. Physical Review A 52.4 (1995):

Shor, P. W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26.5 (aug 1997): 1484–1509.

Simon, D. R. 1997. On the power of quantum computation. SIAM Journal on Computing 26.5 (1997): 1474–1483.

Smolin, J. A. and DiVincenzo, D. P. 1996. Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate. Physical Review A - Atomic, Molecular, and Optical Physics 53.4 (1996): 2855–2856.

Temme, K., Bravyi, S., and Gambetta, J. M. 2017. Error Mitigation for Short-Depth Quantum Circuits. Physical Review Letters 119.18 (nov 2017):

Terhal, B. M. and DiVincenzo, D. P. 2004. Adptive quantum computation, constant depth quantum circuits and arthur-merlin games. Quantum Information and Computation 4.2 (may 2004): 134–145.

Thapliyal, H. and Ranganathan, N. 2013. Design of efficient reversible logic-based binary and BCD adder circuits. ACM Journal on Emerging Technologies in Computing Systems 9.3 (dec 2013):

Thapliyal, H., Varun, T. S., Munoz-Coreas, E., Britt, K. A., and Humble, T. S. 2018. Quantum circuit designs of integer division optimizing T-count and T-depth. In Proceedings - 2017 IEEE International Symposium on Nanoelectronic and Information Systems, iNIS 2017, volume 2018-Febru, pp. 123–128. : Institute of Electrical and Electronics Engineers Inc.

Torlai, G., Mazzola, G., Carrasquilla, J., Troyer, M., Melko, R., and Carleo, G. 2018. Neural-network quantum state tomography. Nature Physics 14.5 (may 2018): 447–450.

Trisetyarso, A. and Van Meter, R. 2010. Circuit design for a measurement-based quantum carry-lookahead adder. International Journal of Quantum Information 8.5 (mar 2010): 843–867.

Van Meter, R., Munro, W. J., Nemoto, K., and Itoh, K. M. 2008. Arithmetic on a distributed-memory quantum multicomputer. ACM Journal on Emerging Technologies in Computing Systems 3.4 (jul 2008):

Vedral, V., Barenco, A., and Ekert, A. 1996. Quantum networks for elementary arithmetic operations. Physical Review A - Atomic, Molecular, and Optical Physics 54.1 (nov 1996): 147–153.

Wang, F., Luo, M., Li, H., Qu, Z., and Wang, X. 2016. Improved quantum ripple-carry addition circuit. Science China Information Sciences 59.4 (apr 2016):

Watson, T. F., Philips, S. G. J., Kawakami, E., Ward, D. R., Scarlino, P., Veldhorst, M., Savage, D. E., Lagally, M. G., Friesen, M., Coppersmith, S. N., Eriksson, M. A., Vandersypen, L. K. M. K., J Philips, S. G., Kawakami, E., Ward, D. R., Scarlino, P., Savage, D. E., Lagally, G., Friesen, M., Coppersmith, S. N., and Vandersypen, L. K. M. K. 2018. A programmable two-qubit quantum processor in silicon. Nature 555.7698 (feb 2018): 633–637.

Wiebe, N. and Roetteler, M. 2016. Quantum arithmetic and numerical analysis using repeat-until-success circuits. Technical Report 1-2.

Wille, R., Soeken, M., and Drechsler, R. 2010. Reducing the number of lines in reversible circuits. In Proceedings - Design Automation Conference, pp. 647–652. :

Wright, K., Beck, K. M., Debnath, S., Amini, J. M., Nam, Y., Grzesiak, N., Chen, J. S., Pisenti, N. C., Chmielewski, M., Collins, C., Hudek, K. M., Mizrahi, J., Wong-Campos, J. D., Allen, S., Apisdorf, J., Solomon, P., Williams, M., Ducore, A. M., Blinov, A., Kreikemeier, S. M., Chaplin, V., Keesan, M., Monroe, C., and Kim, J. 2019. Benchmarking an 11-qubit quantum computer. (mar 2019):

Yang, G., Song, X., Hung, W. N., and Perkowski, M. A. 2008. Bi-directionalsynthesis of 4-bit reversible circuits. Computer Journal 51.2 (mar 2008): 207–215.

Zalka, C. 2006. Shor's algorithm with fewer (pure) qubits. Technical report.

Zhang, X., Xiang, H., and Xiang, T. 2019. An efficient quantum circuits optimizing scheme compared with QISKit (Short Paper). Technical report.

Biography

Naphan Benchasattabuse was born in Bangkok on December, 1994. He graduated from Triam Udom Suksa school and then went to Chulalongkorn University where he received B.Eng in computer engineering. In 2019, he won first place in IBM Quantum Challenge 2019. His field of interest includes various topics in quantum computing, algorithm, web development, and high availability system.

List of Publications

Benchasattabuse, N., Chongstitvatana, P., & Aporntewan, C. (2018). Quantum Rough Counting and Its Application to Grover's Search Algorithm. In 2018 3rd International Conference on Computer and Communication Systems, ICCCS 2018 (pp. 344–348). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CCOMS.2018.8463331