Quantum Algorithms for Distinguishing Unitary Operators

By

Shanu

Department of Computer science

Indraprastha Institute of InformationTechnology

A dissertation submitted to the Indraprastha Institute of Information Technology in accordance with the requirements of the degree of MASTER OF TECHNOLOGY in the Faculty of Computer science.

July, 2018

Certificate

This is to certify that the thesis titled Quantum Algorithms for Distinguishing Unitary Operators being submitted by Shanu to the Indraprastha Institute of Information Technology Delhi, for the award of the Master of Technology, is an original research work carried out by him under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree. The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree/diploma.

July, 2018

Dr. Debajyoti Bera

Department of Computer science
Indraprastha Institute of Information Technology
New Delhi 110020

Acknowledgements

I sincerely thank my advisor, Dr. Debajyoti Bera, who has supported me throughout my thesis with his patience and knowledge. He was always available whenever I needed him and always showed me the right direction to proceed in order to achieve the goal. I attribute the level of my Masters degree to his encouragement and effort and without him this thesis, too, would not have been completed or written. One simply could not wish for a better or friendlier supervisor. Also, I must express my very profound gratitude to my parents and to my friends for providing me with unfailing support and continuous encouragement throughout my study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Abstract

Distinguishing between unitary operators is one of the fundamental problems in the field of quantum computing. In the operator identification problem, we are given access to unknown operator U as a black-box that implements either an operator $U1$ or an operator $U2$, where $U1$ and $U2$ are arbitrary unitary operators and their operations are known to us. The goal is to determine whether U is an implementation of $U1$ or $U2$. In this thesis, two different versions of operator identification problem have been studied followed by a generalization. Firstly, we consider the case when an exact implementation of the operation of the operators $U1$ and $U2$ is given to us. We show that amplitude amplification, which is one of the important tools in quantum computing, can be used to design an efficient algorithm to solve this version of operator identification problem without error. But, in the quantum circuit theory, it may not be always possible to implement an arbitrary operator exactly and it may happen that a fabricated circuit implements a close approximation of the desired unitary operator. For the second version of the problem, we consider the case where the approximate implementation of the operation of the operators $U1$ and $U2$ is given to us; once again the goal is to design an algorithm to solve the problem. Finally, we consider a general version of the operator identification problem when the candidate set is of any size, say n. That is, U implements one of the operators present in the candidate set $\{U_1, U_2, ... , U_n\}$ and we have to identify U. We propose novel approaches to solve all these three problems in this thesis.

Contents

Chapter 1

Background:Amplitude Amplification

Amplitude amplification is one of the most popular tools for an algorithm designer in the quantum computing. Amplitude amplification can be used to increase the success probability of a broad class of quantum algorithms. It provides a polynomial speedup over other classical amplifying techniques which have been designed for the same purpose. The goal of this chapter is to revisit the concepts of amplitude amplification and see how amplitude amplification is used to increase the success probability. The notion of amplitude amplification has been described in a slightly different way as presented in the original paper [4]. The formulation of amplitude amplification as shown in this chapter can be directly applied to solve the problem of operator identification in chapter 2.
As a rough outline of this chapter, we begin with the explanation of an amplification of the randomized algorithms. Then we discuss amplitude amplification as a tool to amplify the success probability of a quantum algorithm. Finally, we discuss a de-randomization technique that can be used to increase the success probability up to one.

1.1 Introduction

1.1.1 Amplification of randomized algorithm

Due to the imposed time and memory constraints, randomized algorithms are widely used to get the acceptable solution in the provided time. Since these algorithms work by randomly making decisions, there is a possibility of error in their outcomes. There is a probability associated with the success of a randomized algorithm called the success probability - the probability by which the algorithm outputs the correct answer within

the allotted time.

The probability of success of the randomized algorithm can be quite low. To get the correct output or to improve the success probability of an algorithm, the amplification technique is used. Amplification is an algorithm which is used to increase the probability of getting the correct output. This is done at the cost of the time. Amplification runs the randomized algorithm several times to amplify the chance of success which leads to increase in the runtime of an algorithm. Therefore. if amplitude amplification is applied, then there is a trade-off between the correctness of an algorithm and the time taken by the algorithm to return the outcome.

The simplest way of applying amplification is by running the original randomized algorithm, whose success probability needs to be boosted, several times. The final output is returned depending on the type of the problem for which an algorithm has been designed. For instance, if the problem is a decision problem, then the algorithm is executed several times and the majority of all the outcomes is returned. On the other hand, if its an optimization problem, then the best outcome of all the outcomes obtained during multiple runs is returned. This approach of amplification works for most of the randomized algorithms but requires a large amount of time to return the result. There are many other sophisticated techniques of applying amplification to the randomized algorithms which have been designed to increase the success probability of the algorithm without affecting its runtime much. These techniques are applicable to some of the classes of randomized algorithms [7].

1.1.2 Amplification of quantum randomized algorithm

The amplification techniques including both sophisticated ones and the simple approach of executing the algorithm several times to increase the success probability of the algorithm can also be applied in the quantum computing. In quantum computing, Brassard et al.[4] proposed an approach of boosting the success probability for a quantum algorithm and named it as amplitude amplification. Amplitude amplification is the generalization of Grover's search algorithm. Grover's search algorithm is widely applicable quantum algorithm proposed by L. Grover in 1996[8]. It provides a quadratic speedup over other best-known classical algorithms designed for a broad class of search problems.

To understand the amplitude amplification, let $\mathcal{A}$ be a quantum algorithm that makes no measurement and produces a superposition state $|\psi\rangle$ when applied on some input state $|\chi\rangle$, i.e., $|\psi\rangle = \mathcal{A}|\chi\rangle$. Let p denote the success probability of the algorithm $\mathcal{A}$ when $|\psi\rangle$ is measured using some projective measurement operator, i.e., the algorithm $\mathcal{A}$ gives the correct solution with the probability p. The amplitude amplification can be seen as an algorithm that uses an iterative operator known as Grover's iterator which is formed using $\mathcal{A}$ and $\mathcal{A}^\dagger$ as black-box. Amplitude amplification increases the success probability of algorithm $\mathcal{A}$ roughly by a constant factor on each application of the Grover's iterator. Since the success probability of the algorithm $\mathcal{A}$ is p, therefore $1/p$ is the expected number of runs of the algorithm required to find a solution if we use the simple amplification approach. Amplitude amplification is a method that requires $1/\sqrt{p}$ applications of $\mathcal{A}$ (and $\mathcal{A}^\dagger$) on the average to find the solution. Thus, a quadratic speedup is obtained by the amplitude amplification approach and because of its quadratic speedup, it has become one of the important tools in the quantum computing. Many algorithms use the technique of amplitude amplification to solve the problem.

Grover's search algorithm can be seen as a special case of amplitude amplification in the following manner: set $\mathcal{A} = H^{\otimes n}$ and use $|\chi\rangle = |0^n\rangle$. Therefore $\mathcal{A}|\chi\rangle$ generates a uniform superposition of all possible solutions that is akin to guessing a solution uniformly at random.

1.2 Amplitude Amplification

Let $\mathcal{H}$ be an N-dimensional Hilbert space spanned by the orthonormal computational basis states $B = \{|b_0\rangle, |b_1\rangle, ..., |b_{N-1}\rangle\}$. Consider a two-outcome projective measurement operator defined by $P = \{P^0, P^1\}$: such that 0 and 1 denotes "bad" and "good" state respectively. This projective measurement operator P can be considered as a Boolean function $f : \mathbb{Z} \to \{0, 1\}$, where $f(x) = 1$ denotes that a state $|x\rangle \in \mathcal{H}$ is a good state and $f(x) = 0$ denotes that a state $|x\rangle \in \mathcal{H}$ is a bad state. P can be used to partition the space $\mathcal{H}$ into two sub-spaces, a good subspace and a bad subspace. The subspace spanned by a set of "good" basis state is the good subspace and its orthogonal complement subspace in $\mathcal{H}$ is the bad subspace. Let $\mathcal{A}$ be any quantum algorithm that acts on $\mathcal{H}$, makes no measurements and produces a superposition state $|\psi\rangle$ when applied on some input state $|\chi\rangle$, i.e, $|\psi\rangle = \mathcal{A}|\chi\rangle$. Here $|\psi\rangle$ is a quantum superposition of the good and the bad

states. When we measure the state $|\psi\rangle$ using P and observe a good state then we say the algorithm $\mathcal{A}$ is successful. Suppose p denotes the probability of success of the algorithm $\mathcal{A}$. Amplitude amplification will be used to increase this success probability and we will call p to be an initial success probability of $\mathcal{A}$.

Define $|\psi'^0\rangle = P^0 |\psi\rangle$ and $|\psi'^1\rangle = P^1 |\psi\rangle$. Let $\theta \in [0, \pi/2]$ be such that $\sin^2\theta = p$. For now, consider the case where $p \in (0, 1)$. This lets us define the following normalized states:

$$|\psi^0\rangle = \frac{1}{\cos\theta} |\psi'^0\rangle, \quad |\psi^1\rangle = \frac{1}{\sin\theta} |\psi'^1\rangle$$

First, observe that $|\psi\rangle = \sin\theta |\psi^1\rangle + \cos\theta |\psi^0\rangle$. Define the state $|\overline{\psi}\rangle = \cos\theta |\psi^1\rangle - \sin\theta |\psi^0\rangle$ which is orthonormal to $|\psi\rangle$. Let $\mathcal{H}'$ be the subspace of $\mathcal{H}$ that is spanned by $|\psi^0\rangle$ and $|\psi^1\rangle$. It can be shown that $|\psi\rangle$ and $|\overline{\psi}\rangle$ form another basis for $\mathcal{H}'$.

Fixing any n-qubit state $|\psi\rangle \in \mathcal{H}$ and the two outcome projective measurement operator $\mathrm{P} = \{P^0, P^1\}$ defines a subspace $\mathcal{H}'$ of $\mathcal{H}$ and the othonormal basis $\{|\psi^1\rangle, |\psi^0\rangle\}$ for $\mathcal{H}'$. $\{|\psi\rangle, |\overline{\psi}\rangle\}$ form another basis for $\mathcal{H}'$. The amplitude amplification is the process of repeatedly applying Grover's iterator $G_{\alpha,\beta}$ that is constructed as the composition of two operators for $0 \leq \alpha, \beta < 2\pi$ as follows:

$$G_{\alpha,\beta} = -GI_\alpha GM_\beta, \qquad where \quad GI_\alpha = I - (\,1 - e^{\iota\alpha}\,)\,|\psi\rangle\langle\psi|, \quad and \quad GM_\beta = I - (\,1 - e^{\iota\beta}\,)\,P^1$$

Lemma 1. *GI_α and GI_β are the unitary operators.*

Proof. We have $GI_\alpha = I - (\,1 - e^{\iota\alpha}\,)\,|\psi\rangle\langle\psi|$ and $GM_\beta = I - (\,1 - e^{\iota\beta}\,)\,P^1$. Corresponding reversible operators are $GI_\alpha^\dagger = I - (\,1 - e^{-\iota\alpha}\,)\,|\psi\rangle\langle\psi|$ and $GM_\beta^\dagger = I - (\,1 - e^{-\iota\beta}\,)\,P^1$. Simple algebra shows that $GI_\alpha^\dagger \cdot GI_\alpha = I$ and $GM_\beta^\dagger \cdot GM_\beta = I$. It follows that operators GI_α and GI_β are the unitary operators. Note that operator P^1 is an orthogonal projector so, $P^{1\dagger} = \mathrm{P}^1$ and $P^1 \,.\, P^1 = \mathrm{P}^1$.

□

Let $|\Phi\rangle \in \mathcal{H}$ be some pure state. Every state $|\Phi\rangle$ has a decomposition $|\Phi\rangle = \sin\phi |\psi^1\rangle + \cos\phi |\psi^0\rangle$ such that $\phi \in [0\ ,\ \pi/2]$. Let $0 < a < 1$; a $= \sin^2\phi$ denotes the probability of observing a good state when $|\Phi\rangle$ is measured using P. Now we will study the action of operator $G_{\pi,\pi}$ on $|\Phi\rangle$ for $\alpha = \beta = \pi$ and this leads to the following lemma.

Lemma 2. *For $\alpha = \beta = \pi$, $G_{\pi,\pi}$ rotates any $|\Phi\rangle \in \mathcal{H}$ by angle 2θ towards $|\psi^1\rangle$. If we measure the $G_{\pi,\pi}|\Phi\rangle$ using P, the probability of observing a good state is $\sin^2(2\theta+\phi)$.*

Proof. We have $GI_\pi = I - 2|\psi\rangle\langle\psi|$ and $GM_\pi = I - 2P^1$. First note that, $P^1|\psi^1\rangle = |\psi^1\rangle$ and $P^1|\psi^0\rangle = 0$. $|\psi^1\rangle$ and $|\psi^0\rangle$ can be written in the form of the basis $\{|\psi\rangle, |\overline{\psi}\rangle\}$ as $|\psi^1\rangle = \sin\theta|\psi\rangle + \cos\theta|\overline{\psi}\rangle$ and $|\psi^0\rangle = \cos\theta|\psi\rangle - \sin\theta|\overline{\psi}\rangle$. Therefore, we can easily convert one basis to another basis of subspace $\mathcal{H}'$. To compute the action of $G_{\pi,\pi}$ on any pure state $|\Phi\rangle$, first consider action of GM_π *on* $|\Phi\rangle$ and then consider the action of GI_π *on* $GM_\pi|\Phi\rangle$.

$$\begin{aligned} GM_\pi|\phi\rangle &= (\ I - 2P^1\ )\ (\ \sin\phi|\psi^1\rangle\ +\ \cos\phi|\psi^0\rangle\ ) \\ &= \sin\phi|\psi^1\rangle\ +\ \cos\phi|\psi^0\rangle - 2\sin\phi|\psi^1\rangle \\ &= \cos\phi|\psi^0\rangle - \sin\phi|\psi^1\rangle \end{aligned}$$

The operator GM_π performs reflection through the axis defined by the vector $|\psi^0\rangle$ of any pure state $|\Phi\rangle \in \mathcal{H}$ in the subspace $\mathcal{H}'$.

We can rewrite $GM_\pi|\phi\rangle$ in the form of $\{|\psi\rangle, |\overline{\psi}\rangle\}$ basis as follows :

$$\begin{aligned} GM_\pi|\phi\rangle &= \cos\phi\ (\ \cos\theta|\psi\rangle\ -\ \sin\theta|\overline{\psi}\rangle\ ) - \sin\phi\ (\ \sin\theta|\psi\rangle\ +\ \cos\theta|\overline{\psi}\rangle\ ) \\ &= (\ \cos\phi.\cos\theta - \sin\phi.\sin\theta\ )\ |\psi\rangle - (\ \cos\phi.\sin\theta + \sin\phi.\cos\theta\ )\ |\overline{\psi}\rangle \\ &= \cos(\theta+\phi)\ |\psi\rangle - \sin(\theta+\phi)\ |\overline{\psi}\rangle \end{aligned}$$

Now, consider the action of GI_π *on* $GM_\pi|\Phi\rangle$

$$\begin{aligned} -G_{\pi,\pi}|\Phi\rangle = GI_\pi GM_\pi|\Phi\rangle &= GI_\pi(\ \cos(\theta+\Phi)\ |\psi\rangle - \sin(\theta+\Phi)\ |\overline{\psi}\rangle\ ) \\ &= (\ I - 2|\psi\rangle\langle\psi|\ )\ (\ \cos(\theta+\Phi)\ |\psi\rangle - \sin(\theta+\Phi)\ |\overline{\psi}\rangle\ ) \\ &= \cos(\theta+\Phi)\ |\psi\rangle - \sin(\theta+\Phi)\ |\overline{\psi}\rangle - 2\cos(\theta+\Phi)\ |\psi\rangle \\ G_{\pi,\pi}|\Phi\rangle &= \cos(\theta+\Phi)\ |\psi\rangle + \sin(\theta+\Phi)\ |\overline{\psi}\rangle \end{aligned}$$

The operator GI_π performs reflection through the axis defined by the vector $|\psi\rangle$ in the subspace $\mathcal{H}'$.

$G_{\pi,\pi}\ |\Phi\rangle$ can be rewritten in the form of $\{|\psi^1\rangle, |\psi^0\rangle\}$ basis as follows:

$$\begin{aligned} G_{\pi,\pi}|\Phi\rangle &= \cos(\theta+\Phi)\ (\ \sin\theta|\psi^1\rangle\ +\ \cos\theta|\psi^0\rangle\ ) + \sin(\theta+\Phi)\ (\ \cos\theta|\psi^1\rangle\ -\ \sin\theta|\psi^0\rangle\ ) \\ &= \{\ \cos(\theta+\Phi).\sin\theta + \sin(\theta+\Phi).\cos\theta\ \}\ |\psi^1\rangle + \{\ \cos(\theta+\Phi).\cos\theta - \sin(\theta+\Phi).\sin\theta\ \}\ |\psi^0\rangle \\ &= \sin(2\theta+\Phi)\ |\psi^1\rangle + \cos(2\theta+\Phi)\ |\psi^0\rangle \end{aligned}$$

□

It follows that applying $G_{\pi,\pi}$, m times for some integer $m \geq 0$, rotates the state $|\Phi\rangle$ by an angle $2m\theta$ towards $|\psi^1\rangle$. The probability of observing a good state when $G^m_{\pi,\pi}|\Phi\rangle$ is measured using P is $\sin^2(2m\theta + \phi)$. Similar results can be found in the book by Kaye et al.[11]. Theorem 1 follows.

Theorem 1. *Given a quantum algorithm $\mathcal{A}$ that makes no measurement and produces a superposition state $|\psi\rangle$ when applied on some input state $|\chi\rangle$, i.e, $|\psi\rangle = \mathcal{A}|\chi\rangle$. Define two outcome projective measurement operator $P = \{P^0, P^1\}$. Let $0 < p < 1$ denotes the probability of observing the good state when $|\psi\rangle$ is measured using P and $\theta \in [0, \pi/2]$ be the angle such that $\sin^2\theta = p$. Consider any state $|\Phi\rangle \in \mathcal{H}$ and $\phi \in [0, \pi/2]$ be such that $\sin^2\phi$ denotes the probability of the observing good state when $|\Phi\rangle$ is measured using P. Then for any integer $m \geq 0$, the probability of observing the good state when $G^m_{\pi,\pi}|\Phi\rangle$ is measured using P is $\sin^2(2m\theta + \phi)$.*

Corollary 1. *When $\phi = \theta$, the state that is used to define the operator $G_{\pi,\pi}$ is the same as the state on which $G_{\pi,\pi}$ is applied, i.e, $|\Phi\rangle = |\psi\rangle$. Hence, the probability of observing a good state, when $G^m_{\pi,\pi}|\psi\rangle$ is measured using P is $\sin^2((2m+1)\theta)$.*

Let $\theta = \phi$ for the remaining part of the chapter. Theorem 1 only states that the m applications of the operator $G_{\pi,\pi}$ increase the success probability from $\sin^2\theta$ to $\sin^2((2m+1)\theta)$. It tells nothing about the number of iterations m needed to get the appropriate success probability. So, it can be asked that how many applications of $G_{\pi,\pi}$ is needed to find the good state with the high probability, i.e. what is the appropriate value of m to achieve the good state. Another question that may come to mind is whether it is possible to find the good state with certainty and if it is, then how to achieve it.
To answer the first question of how many applications of $G_{\pi,\pi}$ is needed to find the good state with the high probability, consider the following result from Brassed et al. [4]:

Result(Quadratic speedup):
Given a quantum algorithm $\mathcal{A}$ that makes no measurement and produces a superposition state $|\psi\rangle$ when applied on some input state $|\chi\rangle$, i.e, $|\psi\rangle = \mathcal{A}|\chi\rangle$. Define a two outcome projective measurement operator P $= \{P^0, P^1\}$. Let $0 < p \leq 1$ denote the probability of observing a good state when $|\psi\rangle$ is measured using P and $\theta \in (0, \pi/2]$ be the angle such

that $\sin^2\theta = p$. Set $m = \lfloor \pi/4\theta \rfloor$ and if we measure the state $G^m_{\pi,\pi}|\psi\rangle$ using P then we observe a good state with probability of at least $max(p, 1-p)$.

The following subsection answers the second question and explains one of the possible ways to improve the success probability to certainty. The number of applications required to achieve this task is also described.

1.2.1 Improving success probability to certainty

Brassard et al.[4] (same paper in which amplitude amplification has been proposed) suggested two optimal de-randomization techniques to improve the success to certainty. This subsection will explain one of those two techniques proposed in the paper, although other approaches are also possible.

From Corollary 1, we know that after m applications, the probability of observing a good state is $\sin^2((2m+1)\theta)$. Our goal is to achieve the good state with the high probability i.e., we want $\sin^2((2m+1)\theta)$ close to one. Therefore, we need to have $(2m+1)\theta$ close to $\pi/2$. Setting $m = \lfloor \pi/4\theta - 1/2 \rfloor$ makes $(2m+1)\theta$ close to $\pi/2$. Note that we are taking floor because m (the number of iterations) should be an integer. If $\pi/4\theta - 1/2$ is an integer then we observe a good state with certainty, otherwise we observe a good state with high probability when $G^m_{\pi,\pi}|\psi\rangle$ is measured.

Let $\overline{\theta} = \pi/(4M+2)$, where $M = \lceil \pi/4\theta - 1/2 \rceil$. Consider a quantum algorithm $\mathcal{B}$ such that it succeeds with initial probability $\sin^2(\overline{\theta})$ (say $\overline{p}$). If we can construct such algorithm and apply amplitude amplification on it instead of on algorithm $\mathcal{A}$, then we can improve the success probability to certainty after M applications of amplitude amplification.

Given an algorithm $\mathcal{A}$ that succeeds with an initial probability $p = \sin^2\theta$, we can construct an algorithm $\mathcal{B}$ that succeeds with an initial probability $\overline{p} = \sin^2\overline{\theta}$ that is slightly smaller than p. One possible way to design $\mathcal{B}$ is as follows: let $\mathcal{C}$ be a single qubit quantum algorithm which converts state $|0\rangle$ into a $\sqrt{1-\overline{p}/p}\,|0\rangle + \sqrt{\overline{p}/p}\,|1\rangle$ superposition state. Consider the algorithm $\mathcal{B}$ as applying both $\mathcal{A}$ and $\mathcal{C}$ in parallel on input state $|\chi\rangle\,|0\rangle$. Define good states as those states in which an outcome of $\mathcal{A}$ is a good state and an outcome of $\mathcal{C}$ is $|1\rangle$.

We can use $\mathcal{B}$ and $\mathcal{B}^\dagger$ to define an operator $G_{\pi,\pi}$. Note that in each iteration of amplitude amplification, the operator $G_{\pi,\pi}$ is applied once and one application of operator $G_{\pi,\pi}$ makes two calls to the black-box. One call is made to $\mathcal{A}$ by an operator $\mathcal{B}$ and another

to $\mathcal{A}^\dagger$ by an operator $\mathcal{B}^\dagger$. In this way, total of $2M$ calls are made to $\mathcal{A}$ and $\mathcal{A}^\dagger$. Immediate theorem 2 follows.

Theorem 2. *Given a quantum algorithm $\mathcal{A}$ as a black-box that makes no measurement and produces a superposition state $|\psi\rangle$ when applied on some input state $|\chi\rangle$, i.e, $|\psi\rangle = \mathcal{A}|\chi\rangle$. Define two outcome projective measurement operator $P = \{P^0, P^1\}$. Let $0 < p < 1$ denote the probability of observing a good state when $|\psi\rangle$ is measured using P and $\theta \in [0, \pi/2]$ be an angle such that $\sin^2\theta = p$. We can find a good state with certainty using $2M$ number of applications of $\mathcal{A}$ and $\mathcal{A}^\dagger$, where $M = \lceil \pi/4\theta - 1/2 \rceil$.*

Case 1. *If the initial success probability $p = 1$ or $\theta = \pi/2$ then $M = 0$. As $M = 0$, amplitude amplification does not change the success probability. We observe a good state with certainty.*

Case 2. *If the initial success probability $p = 0$ or $\theta = 0$ then for any integer $M \geq 0$, amplitude amplification does not change the success probability. We observe a bad state with certainty.*

To summarize, if we have a quantum algorithm that makes no measurement and succeeds with some non-zero probability then, amplitude amplification can be used to improve this success probability. It is even possible to improve the success probability up to one. If the initial success probability of the quantum algorithm is zero then the application of amplitude amplification cannot improve the success probability.

Chapter 2

Amplitude Amplification For Exact Operator identification

The problem of distinguishing two unitary operators is a well studied problem in the field of quantum computing. In this chapter, an efficient novel approach to solve this problem without any error has been introduced which uses the approach of amplitude amplification explained in the previous chapter.

As a rough outline of this chapter, we begin with the introduction of the problem of distinguishing two unitary operators which is named as the operator identification problem followed by the review of work done to distinguish two operators. Next, we discuss how the amplitude amplification can be used to solve the problem of operator identification. An efficient algorithm has been designed that solves the problem without any error. Also, an analysis has been done on the number of queries and the number of the qubits needed by the algorithm.

2.1 Introduction

Distinguishing of two non-orthogonal quantum states is one of the most fundamental problems in the quantum information theory[2, 6, 10, 12]. This problem is known as the state identification problem. In a typical scenario, the state identification problem can be defined as follows: Given an unknown quantum state $|\phi\rangle$ that is chosen from a set of two non-orthogonal quantum states $\{|\phi_1\rangle, |\phi_2\rangle\}$, determine whether $|\phi\rangle$ is $|\phi_1\rangle$ or $|\phi_2\rangle$ with the high probability.

If the states $|\phi_1\rangle$ and $|\phi_2\rangle$ are orthonormal states then the given unknown state can always be discriminated without any error. This can be done using a simple procedure:

Define the measurement operators $P = \{P_a, P_b\}$, where $P_a = |\phi_1\rangle\langle\phi_1|$ and $P_b = I - |\phi_1\rangle\langle\phi_1|$ and its corresponding outcomes are a and b respectively. Measure the state $|\phi\rangle$ using the operator P. If the outcome is a then the unknown state is regarded as state $|\phi_1\rangle$ otherwise it is considered as state $|\phi_2\rangle$. It can be shown easily that if $|\phi\rangle = |\phi_1\rangle$ then the probability of observing an outcome a is one and if $|\phi\rangle = |\phi_2\rangle$ then the probability of observing outcome a is zero, when $|\phi\rangle$ is measured using P. Therefore, using this simple method, the states can be identified with certainty for the case when the states are orthonormal.

The other case is when the states $|\phi_1\rangle$ and $|\phi_2\rangle$ are not orthonormal. In this case, we cannot find such measurement operator that could distinguish non-orthogonal states. This is because, the state $|\phi_1\rangle$ can be decomposed in terms of the state $|\phi_2\rangle$ i.e., it can be divided into non-zero component of $|\phi_2\rangle$ and a component orthonormal to state $|\phi_2\rangle$. In fact, it is well known that two non-orthogonal states cannot be discriminated without an error unless you are provided with an infinite number of copies of the unknown state [10, 11].

An important problem related to the state identification problem is an operator identification problem[10]. Typically an operator identification problem is defined as follows: Given an unknown operator $\mathcal{U}$ as a black-box which implements either an operator $\mathcal{U}1$ or an operator $\mathcal{U}2$, the goal is to determine whether an unknown operator $\mathcal{U}$ is an implementation of $\mathcal{U}1$ or $\mathcal{U}2$.

Consider $A(\mathcal{U})$ to be a unitary operator that is constructed using an unknown operator $\mathcal{U}$ along with some other known operators including $\mathcal{U}1$ or $\mathcal{U}2$. Let $A1 = A(\mathcal{U}1)$ and $A2 = A(\mathcal{U}2)$. Operator identification problem can be reduced into state identification problem: Choose an input state say $|\alpha\rangle$. Identify whether the unknown state $A|\alpha\rangle$ is $A1|\alpha\rangle$ or $A2|\alpha\rangle$. In contrast to the state identification problem, a perfect discrimination between two different unitary operators is possible. This is due to the flexibility of choosing an input state and designing such operator A. A perfect discrimination between the operators can be achieved by taking a suitable entangled state as input and then applying an unknown unitary operation in parallel[1, 5, 10]. A sequential method has also been proposed that applies $\mathcal{U}$ in a sequential manner on a suitably chosen non-entangled state[6].

2.2 Problem Statement

In the previous section, we introduced the operator identification problem. In this section, we define the problem formally.

Definition 1 (Operator identification problem)**.** *Given an operator unknown $\mathcal{C}$ as a black-box which implements either operator $\mathcal{C}1$ or $\mathcal{C}2$, where the operation for $\mathcal{C}1$ and $\mathcal{C}2$ are known to us and $\mathcal{C}1 \neq e^{i\alpha}\mathcal{C}2$ for any α. The goal of the operator identification problem is to determine whether $\mathcal{C} = \mathcal{C}1$ or $\mathcal{C} = \mathcal{C}2$.*

2.3 Related Work

Acin[1] studied the problem of distinguishing two unitary operators and provided a fidelity-like function that measures the orthogonality (or closeness) between quantum operators. The closeness between the operators reflects their statistical distinguishability. They used sophisticated metrics based on Fubini-Study and Bures to measure the closeness between the operators. They also showed that any two unitary operators can be perfectly discriminated by applying the operators in parallel on some well-chosen entangled quantum state.

Duan et al.[6], in their work, showed how to perfectly discriminate two unitary operators. They applied an unknown operator $\mathcal{C}$ in sequence with some other known operator (say X) multiple times on a well chosen non-entangled state. The operator X is independent of $\mathcal{C}$ but it can depend on known operators $\mathcal{C}1$ and $\mathcal{C}2$. They also proved some upper bound on number of iterations needed to perfectly discriminate the operators. They considered one iteration as an application of the unknown operator $\mathcal{C}$ followed by some known unitary operator.

Kawachi et al.[10] explored the complexity of the discrimination problem for general quantum unitary operators. A single application of an unknown operator $\mathcal{C}$ is called a *query*. The complexity of the problem was studied in terms of the number of queries needed to solve the problem. Note that the number of queries depends on the closeness between the operators. One notion of closeness is explained later in this chapter. The definition of the closeness used by us is same as the one used by Kawachi et al.[10]. They also described an algorithm to solve the problem in the bounded error setting and proved an upper bound on the number of queries by showing a trade-off between the number of

queries and the success probability. They claimed that the upper bound found by them is not more than bounds of any other known algorithm for the problem and showed that this bound is tight up to a possible constant factor when we need the success probability of *at least* 2/3.

In the following sections, we introduce an algorithm that uses amplitude amplification as a tool to solve the problem of operator identification. The analysis of the number of queries and the number of qubits needed by the algorithm has been done. We show that the number of queries needed by the algorithm designed by us is at most one more than the number of queries needed by the algorithm given by Kawachi et al.[10] (best known upper bound) to solve the problem without any error. The proposed algorithm requires lesser number of qubits as compared to the algorithm used by Kawachi et al.[10]. The number of qubits is reduced by a factor of the number of queries needed by the algorithm used by Kawachi et al.[10] to solve the problem. All the comparisons have been done by setting the error to be zero in the algorithm used by Kawachi et al.[10].

2.4 Amplitude Amplification For Operator Identification

We will use amplitude amplification as a tool to solve the operator identification problem. First, recall amplitude amplification from chapter 1. Given an algorithm A that makes no measurement and produces some output state $|\psi\rangle$ when applied on some input state. Define a two outcome projective measurement operator P in the similar way as defined in chapter 1. Let p denotes the probability of getting the desired outcome when state $|\psi\rangle$ is measured using P. This probability of observing the desired outcome is known as the success probability and p is the initial success probability of the algorithm A. If $p > 0$ then the application of amplitude amplification on the algorithm can improve this success probability p to one. When $p = 0$ then amplitude amplification has no effect on this success probability. Amplitude amplification can be considered as repeatedly applying a unitary operator on the output state $|\psi\rangle$. This unitary operator is defined using the algorithm A and the measurement operator P. Each iteration of this operator increases the success probability by a constant factor.

In operator identification problem, an unknown unitary operator is given as a black-box. It is guaranteed that this given black-box implements one of the known unitary

operators $\mathcal{C}1$ or $\mathcal{C}2$. Our approach to solving the problem of operator identification is as follows: Consider a given black-box $\mathcal{C}$ to be an algorithm. Define two outcome projective measurement operator P and let its possible outcomes be 0 and 1. We define P in such a way that if $\mathcal{C} = \mathcal{C}1$ then the probability of getting outcome 1 is zero, i.e, $p = 0$ and if $\mathcal{C} = \mathcal{C}2$ then the probability of outcome 1 is non-zero, i.e, $p > 0$. Amplitude amplification is applied on the state $\mathcal{C}|\chi\rangle$ for some input state $|\chi\rangle$. If $\mathcal{C} = \mathcal{C}1$ then $p = 0$. In this case, amplitude amplification has no effect on the success probability. If $\mathcal{C} = \mathcal{C}2$ then $p > 0$. In this case, the appropriate number of applications of amplitude amplification can improve the success probability to one. We have the flexibility to choose an input state in case of operator identification problem. The input state is chosen in such a way that it maximizes the initial success probability p when $\mathcal{C} = \mathcal{C}2$.

Let the state produced by the given unknown operator $\mathcal{C}$ when applied on some input state $|\chi\rangle$ be $|\psi\rangle$, i.e., $|\psi\rangle = \mathcal{C}|\chi\rangle$. Say $|\psi_1\rangle = \mathcal{C}1|\chi\rangle$ and $|\psi_2\rangle = \mathcal{C}2|\chi\rangle$. Define two outcome projective measurement operator $P = \{P^0, P^1\}$, where $P^0 = |\psi_1\rangle\langle\psi_1|$ and $P^1 = I - |\psi_1\rangle\langle\psi_1|$. The superscripts 0 and 1 denote "bad" and "good" state respectively. This definition is analogous to the definitions used in amplitude amplification as there is a fixed state $|\psi\rangle$ and we have defined a two outcome projective measurement. In the remaining part of this section, we will see what is the probability of measuring a good state when $|\psi\rangle$ is measured using P for the two possible candidates of $|\psi\rangle$. We will call this probability as the initial success probability since this terminology is used in amplitude amplification. Lemma 3 follows:

Lemma 3. *Let $|\psi\rangle = \mathcal{C}|\chi\rangle$. If we measure $|\psi\rangle$ using P then the probability of observing a good state is 0 if $\mathcal{C} = \mathcal{C}1$ and $1 - |\langle\psi_1|\psi_2\rangle|$ if $\mathcal{C} = \mathcal{C}2$.*

Proof. We will consider both the cases of $\mathcal{C} = \mathcal{C}1$ and $\mathcal{C} = \mathcal{C}2$.

Case 1. *In the case when $\mathcal{C} = \mathcal{C}1$, we have $|\psi\rangle = |\psi_1\rangle$*

The probability of observing a good state corresponding to P^1 is $||P^1|\psi_1\rangle|| = ||(|\psi_1\rangle - |\psi_1\rangle\langle\psi_1|)|\psi_1\rangle|| = 0$.

Case 2. *In the case when $\mathcal{C} = \mathcal{C}2$, we have $|\psi\rangle = |\psi_2\rangle$*

The probability of observing the good state in this case:

$$\begin{aligned} ||P^1 |\psi_2\rangle|| &= ||(I - |\psi_1\rangle \langle\psi_1|) |\psi_2\rangle|| \\ &= || \, |\psi_2\rangle - \langle\psi_1|\psi_2\rangle |\psi_1\rangle || \\ &= 1 - |\langle\psi_1|\psi_2\rangle| \end{aligned}$$

□

Lemma 3 tells about the initial success probability in both the cases when $\mathcal{C} = \mathcal{C}1$ and $\mathcal{C} = \mathcal{C}2$. Next step is to define an iterative operator (known as Grover's iterator) for amplitude amplification. Grover's iterator G can be defined as follows:

$$G_{\pi,\pi} = -GI_\pi GM_\pi, \qquad where \quad GI_\pi = [\, \mathcal{C} \, (\, I - 2\,|\chi\rangle\langle\chi|\,)\, \mathcal{C}^\dagger \,] \quad and \quad GM_\pi = [\, I - 2P^1 \,]$$

Let $p = 1 - |\langle\psi_1|\psi_2\rangle|$ and $\theta = \sin^{-1}(\sqrt{p})$. Note that $p > 0$ because $\mathcal{C}1 \neq e^{\iota\alpha}\mathcal{C}2$, for any α. Here, Grover's iterator has been defined in the same way as defined for amplitude amplification. To see the effect of operator $G_{\pi,\pi}$ on $|\psi\rangle$ for both the possible values of $|\psi\rangle$, consider the following lemma:

Lemma 4. *Let $M = \lceil \pi/4\theta - 1/2 \rceil$ and $|\psi\rangle = \mathcal{C}\,|\chi\rangle$. If we apply $G_{\pi,\pi}$ M times on $|\psi\rangle$ and measure the state $G^M_{\pi,\pi}\,|\psi\rangle$ using P then we can identify whether $\mathcal{C} = \mathcal{C}1$ or $\mathcal{C} = \mathcal{C}2$ with certainty. If we observe a good state then $\mathcal{C} = \mathcal{C}1$ otherwise $\mathcal{C} = \mathcal{C}2$.*

Proof. We will consider both the cases of $\mathcal{C} = \mathcal{C}1$ and $\mathcal{C} = \mathcal{C}2$.

Case 1. *In the case when $\mathcal{C} = \mathcal{C}1$, we have $|\psi\rangle = |\psi_1\rangle$*
Therefore, $GI_\pi = [I - 2\,|\psi_1\rangle\langle\psi_1|\,]$ and $GM_\pi = [\, I - 2P^1 \,]$. The initial probability of observing a good state when $|\psi_1\rangle$ is measured is 0. For any integer $M \geq 0$, amplitude amplification does not change the success probability and we observe a bad state with certainty.

Case 2. *In the case when $\mathcal{C} = \mathcal{C}2$, we have $|\psi\rangle = |\psi_2\rangle$*
Therefore, $GI_\pi = [I - 2\,|\psi_2\rangle\langle\psi_2|\,]$ and $GM_\pi = [\, I - 2P^1 \,]$. Let $p = 1 - |\langle\psi_1|\psi_2\rangle| > 0$ be the initial probability of observing a good state when $|\psi_2\rangle$ is measured and choose θ such that $\sin^2\theta = p$. From theorem 2, for $M = \lceil \pi/4\theta - 1/2 \rceil$, if we compute and measure the state $G^M_{\pi,\pi}\,|\psi_2\rangle$ then we observe the good state with certainty.

□

2.4.1 Generate initial quantum state $|\chi\rangle$

We want an initial quantum state $|\chi\rangle$ such that the number of queries to the algorithm $\mathcal{C}$ is minimized. Note that the number of queries only depends on θ, where $\theta = \sin^{-1}(\sqrt{1 - |\langle\chi| \mathcal{C}1^{\dagger}\mathcal{C}2 |\chi\rangle|})$. As θ becomes larger, the number of queries becomes smaller. Therefore, our goal is to find the quantum state $|\chi\rangle$ that maximizes $\sin^{-1}(\sqrt{1 - |\langle\chi| \mathcal{C}1^{\dagger}\mathcal{C}2 |\chi\rangle|})$. The technique used to find the quantum state $|\chi\rangle$ that maximizes $\sin^{-1}(\sqrt{1 - |\langle\chi| \mathcal{C}1^{\dagger}\mathcal{C}2 |\chi\rangle|})$ has been shown in the work done by Kawachi et al.[10]. Note that the above maximization problem is same as the following minimization problem:

$$\min_{|\chi\rangle} |\langle\chi| \mathcal{C}1^{\dagger} \mathcal{C}2 |\chi\rangle| = \min_{|\chi\rangle} |\langle\chi| \mathcal{V} |\chi\rangle|, \quad where\ \mathcal{V} = \mathcal{C}1^{\dagger} \mathcal{C}2 \tag{2.1}$$

Definition 2 ($\Delta(\mathcal{V})$)**.** *Let $e^{\iota\theta_1}, e^{\iota\theta_2}, ..., e^{\iota\theta_n}$ denote the eigen-values of a unitary operator $\mathcal{V}$. If we represent all the eigen-values of $\mathcal{V}$ on a unit complex circle then $\Delta(\mathcal{V})$ is defined as the angle of the smallest length arc containing all the eigenvalues of $\mathcal{V}$.*

Let $e^{\iota\theta_1}, e^{\iota\theta_2}, ..., e^{\iota\theta_n}$ denote the eigen values of $\mathcal{V}$ and the corresponding eigen vectors are denoted by $|v_1\rangle, |v_2\rangle, ... |v_n\rangle$. By spectral theorem, $\mathcal{V}$ can be written in the form of its own eigenbasis:

$$\mathcal{V} = \sum_{j=1}^{n} e^{\iota\theta_j} |v_j\rangle \langle v_j| \tag{2.2}$$

The initial quantum state $|\chi\rangle$ can also be written in the form of the same eigen-basis for some $a_i \in \mathbb{C}$ for, i = 1,2, . . . ,n and $\sum_{i=1}^{n} |a_i|^2 = 1$:

$$|\chi\rangle = \sum_{j=1}^{n} a_j |v_j\rangle \tag{2.3}$$

Using equation (2.2) and (2.3), (2.1) become

$$\min_{\sum_{j=1}^{n} |a_j|^2 = 1} \sum_{j=1}^{n} |a_j|^2 e^{\iota\theta_j} \tag{2.4}$$

Let **OPT($\mathcal{V}$)** denote the optimization problem represented by the equation(2.4). The solution to this optimization problem can be found efficiently as it can be formalized in the following form: If $e^{\iota\theta_1}, e^{\iota\theta_2}, ..., e^{\iota\theta_n}$ are some points on a complex plane, then $\sum_{j=1}^{n} |a_j|^2 e^{\iota\theta_j}$ represents a convex set, where $\sum_{j=1}^{n} |a_j|^2 = 1$. Equation (2.4) is the square of the shortest distance from the origin of the complex plane to the convex set. There are many well-known efficient approaches to solve the problem of finding the shortest distance from

convex polynomial to a point either inside the convex or outside the convex. Therefore, we can use some approach and find the value of $a_i \in \mathbb{C}$ (i = 1,2,...,n) that solve the optimization problem **OPT($\mathcal{V}$)**. Let $\vec{A} = \{\overline{a}_1, \overline{a}_2, ..., \overline{a}_n\}$ *where*, $\overline{a}_i \in \mathbb{C}$ (i = 1,2,...,n), be the solution of **OPT($\mathcal{V}$)**. Therefore, the required state is

$$|\chi\rangle = \sum_{j=1}^{n} \overline{a}_j |v_j\rangle \tag{2.5}$$

The optimization problem formulated in the paper of Kawachi et. al.[10] to find an optimal initial state for their algorithm is same as the problem **OPT($\mathcal{V}$)** formulated in Equation (2.4). Using the solution of this problem, Kawachi et. al.[10] found an optimal initial state for their algorithm which is same as the initial state $|\chi\rangle$ represented in equation (2.5). They showed that $|\chi\rangle$ is an entangled state and proved that corresponding to the entangled state $|\chi\rangle$, $\min_{|\chi\rangle}|\langle\chi| \mathcal{C}1^\dagger \mathcal{C}2 |\chi\rangle| = \cos^2(\Delta(\mathcal{V})/2)$. We have $\theta = \sin^{-1}(\sqrt{1 - |\langle\chi| \mathcal{C}1^\dagger\mathcal{C}2 |\chi\rangle|})$. Therefore, if we use an optimal initial state then $\theta = \Delta(\mathcal{V})/2$.

The number of queries needed by the algorithm depends on the value of $\Delta(\mathcal{V})$ as the number of queries depends on the value of θ that depends on $\Delta(\mathcal{V})$. Thus, $\Delta(\mathcal{V})$ can be used to measure the closeness between two unitary operators $\mathcal{C}1$ and $\mathcal{C}2$. Given two unitary operators $\mathcal{C}1$ and $\mathcal{C}2$, the procedure of generating the input state that optimizes the number of queries needed to solve the operator identification problem, when $\mathcal{C}1$ and $\mathcal{C}2$ are used as candidate operators, is showed in Algorithm 1.

Algorithm 1: Algorithm to generate initial quantum state

input : Operator $\mathcal{C}1$, $\mathcal{C}2$
output: State $|\chi\rangle$
1 $\{e^{\iota\theta_1}, e^{\iota\theta_2}, ..., e^{\iota\theta_n}\}$ ← eigen-values of $\mathcal{C}1^\dagger \mathcal{C}2$
2 $\{|v_1\rangle, |v_2\rangle, ... |v_n\rangle\}$ ← eigen-vectors of $\mathcal{C}1^\dagger \mathcal{C}2$
3 $\{\overline{a}_1, \overline{a}_2, ..., \overline{a}_n\}$ ← Solution of **OPT**($\mathcal{C}1^\dagger \mathcal{C}2$)
4 $|\chi\rangle = \sum_{j=1}^{n} \overline{a}_j |v_j\rangle$
5 return $|\chi\rangle$

2.4.2 Complete Algorithm and performance analysis

The complete algorithm to solve the operator identification problem without any error is shown in Algorithm 2. Line numbers (2-11) correspond to the improvement of the success probability to one as explained in section [1.2.1]. Consider the case when $\Delta(\mathcal{C}_1^\dagger \mathcal{C}_2) >$

π. In this case, we have $\theta > \pi/2$. This condition contradicts with what we need to apply the amplitude amplification. To apply the amplitude amplification to the operator identification problem, we need $\theta \leq \pi/2$. The algorithm given below is designed to work for the case when $\Delta(\mathcal{C}_1^\dagger\ \mathcal{C}_2) \leq \pi$ as it is easy to solve the operator identification problem for the other case when $\Delta(\mathcal{C}_1^\dagger\ \mathcal{C}_2) \geq \pi$ i.e., if $\theta > \pi/2$ using the following result: If $\Delta(\mathcal{C}_1^\dagger\ \mathcal{C}_2) \geq \pi$ then there always exist an initial quantum state $|\chi\rangle$ such that the states $\mathcal{C}1\,|\chi\rangle$ and $\mathcal{C}2\,|\chi\rangle$ are orthonormal[1] and the identification of the orthogonal states can be done using the simple procedure explained in chapter 1. We will consider $\Delta(\mathcal{C}_1^\dagger\ \mathcal{C}_2) \leq \pi$ for the rest of the discussion.

The number of queries needed (application of an unknown operator $\mathcal{C}$) by the proposed algorithm can be examined as follows: One application of $\mathcal{C}$ is being made in line 12 to generate a state $|\psi\rangle$. In line 22, $G_{\pi,\pi}$ is being applied M times, where $M = \left\lceil \frac{\pi}{2\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} - \frac{1}{2} \right\rceil$. One application of $G_{\pi,\pi}$ makes two calls to the black-box: one call to $\mathcal{C}$ and another call to $\mathcal{C}^\dagger$. Therefore, the algorithm 2 makes total of $2M + 1$ calls to the operator $\mathcal{C}$. If the operator $\mathcal{C}$ operates on initial n qubits state then the number of qubits needed by the algorithm is at most $n + 1$.

Kawachi et al.[10] algorithm required $\left\lceil \frac{\pi}{\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} \right\rceil$ queries to solve the operator identification problem without any error. If the operator $\mathcal{C}$ operate on initial n qubits state then the number of qubits needed by the Kawachi et al.[10] algorithm is $n \times \left\lceil \frac{\pi}{\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} \right\rceil$.

It can be seen that the number of queries needed by the algorithm designed by us is at most one more than the number of queries needed by the algorithm given by Kawachi et al.[10] (best known upper bound) to solve the problem without any error. The proposed algorithm requires lesser number of qubits as compared to the algorithm used by Kawachi et al.[10]. The number of qubits is reduced by factor of $\left\lceil \frac{\pi}{\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} \right\rceil$ (the number of queries needed by the algorithm used by Kawachi et al.[10]) to solve the problem.

Algorithm 2: Operator identification

input : $\mathcal{C}$ Operator C as black-bax
$\{\mathcal{C}1, \mathcal{C}2\}$ Candidate set

output: Identify whether $\mathcal{C}$ is $\mathcal{C}1$ or, $\mathcal{C}2$

$|\chi\rangle \leftarrow$ *Algorithm* $1(\mathcal{C}1, \mathcal{C}2)$
if $(\frac{\pi}{2\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} - \frac{1}{2})$ is not integer **then**
  $p = 1 - |\langle\chi| \mathcal{C}1^\dagger\mathcal{C}2 |\chi\rangle|$
  $\overline{m} = \left\lceil \frac{\pi}{2\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} - \frac{1}{2} \right\rceil$
  $\overline{p} = \sin^2(\pi/(\overline{m}+2))$
  Define single qubit unitary operator $\mathcal{B} = |1\rangle\langle 1| + |0\rangle(\sqrt{1-\overline{p}/p}\,\langle 0| + \sqrt{\overline{p}/p}\,\langle 1|)$
  Update $\mathcal{C} \leftarrow$C $\otimes\mathcal{B}$
  Update $\mathcal{C}1 \leftarrow$C1 $\otimes\mathcal{B}$
  Update $\mathcal{C}2 \leftarrow$C2 $\otimes\mathcal{B}$
  Update input state $|\chi\rangle \leftarrow |\chi\rangle \otimes |0\rangle$
end
$|\psi\rangle = \mathcal{C}|\chi\rangle$
$|\psi_1\rangle = \mathcal{C}1|\chi\rangle$
$|\psi_2\rangle = \mathcal{C}2|\chi\rangle$
$P^0 = |\psi_1\rangle\langle\psi_1|$
$P^1 = I - |\psi_1\rangle\langle\psi_1|$
$P = \{P^0, P^1\}$
$GI_\pi = [\ \mathcal{C}\ (\ I - 2|\chi\rangle\langle\chi|\ )\ \mathcal{C}^\dagger\ ]$
$GM_\pi = [\ I - 2P^1\ ]$
$G_{\pi,\pi} = -GI_\pi GM_\pi$
$M = \left\lceil \frac{\pi}{2\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} - \frac{1}{2} \right\rceil$
Outcome $\leftarrow$ Measure the state $G^M_{\pi,\pi}|\psi\rangle$ using P
if Outcome is 1 **then**
  return $\mathcal{C} = \mathcal{C}1$
else
  return $\mathcal{C} = \mathcal{C}2$
end

Theorem 3. *Given an unknown operator $\mathcal{C}$ that implements either an operator $\mathcal{C}1$ or $\mathcal{C}2$, where the operation for $\mathcal{C}1$ and $\mathcal{C}2$ are known to us and $\mathcal{C}1 \neq e^{i\alpha}\mathcal{C}2$ for any α. The above algorithm can identify whether $\mathcal{C} = \mathcal{C}1$ or $\mathcal{C} = \mathcal{C}2$ without error by making $2M+1$ calls to the algorithm $\mathcal{C}$ and $\mathcal{C}^\dagger$, where $M = \left\lceil \frac{\pi}{2\Delta(\mathcal{C}1^\dagger\ \mathcal{C}2)} - \frac{1}{2} \right\rceil$.*

To summarize, amplitude amplification is used to increase the success probability of a quantum algorithm. We used amplitude amplification to design an efficient algorithm to solve the operator identification problem without any error.

Chapter 3

Approximate Operator Identification

In the previous chapter, we introduced an operator identification problem and also proposed an algorithm to solve it. In this chapter, the modified operator identification problem that is named as approximate operator identification problem is explained. An algorithm to solve this new problem has been presented.
As a rough outline of this chapter, we begin with the discussion of what it means to approximate the unitary operation. The algorithm to solve the approximate operator identification problem has been proposed. Also, an analysis on the lower bound of the success probability of the proposed algorithm has been shown.

3.1 Introduction

In chapter 2, we discussed the operator identification problem and designed an efficient algorithm to solve it. To recall, the operator identification problem is defined as: Given an operator $\mathcal{C}$ as a black-box which implements either operator $\mathcal{C}1$ or $\mathcal{C}2$, where the operation of $\mathcal{C}1$ and $\mathcal{C}2$ are known to us and $\mathcal{C}1 \neq e^{i\alpha}\mathcal{C}2$ for any α. The goal is to determine whether $\mathcal{C} = \mathcal{C}1$ or $\mathcal{C} = \mathcal{C}2$. Here, one point to note is that the operation of $\mathcal{C}1$ and $\mathcal{C}2$ are arbitrary unitary operations. In quantum circuit theory, a discrete set of quantum gates is used to implement the unitary operation. This discrete set of gates cannot exactly implement an arbitrary unitary operation. They can only approximate the unitary operations. Therefore, it is not always possible to implement the operations of $\mathcal{C}1$ and $\mathcal{C}2$ exactly. We are just able to approximate its operations.

To understand what it means to approximate a unitary operation, consider U and V to be two unitary operators on the same state space. We want to implement the operation of the operator U but we are able to implement the operator V. Let $E(U, V)$ denote the

error when V is implemented instead of U. We will call this error as an approximation error. The approximation error $E(U, V)$ is defined later in the chapter.

The problem of operator identification can now be redefined as follows: Given an operator $\mathcal{C}$ as a black-box which implements either operator $\mathcal{C}1$ or $\mathcal{C}2$, the aim is to guess whether $\mathcal{C}$ implemented $\mathcal{C}1$ or $\mathcal{C}2$. We don't have an exact implementation of $\mathcal{C}1$ and $\mathcal{C}2$ but we are only able to approximate the operations of $\mathcal{C}1$ and $\mathcal{C}2$. We call this modified operation identification problem as approximate operator identification problem. To the best of our knowledge, no work has been done by now to solve the approximate operator identification problem. In this chapter, we present an algorithm to solve this problem. The proposed algorithm uses only one query to the black-box $\mathcal{C}$ to guess whether $\mathcal{C} = \mathcal{C}1$ or, $\mathcal{C} = \mathcal{C}2$ with some probability. We also find the lower bound on the success probability and show how it depends on the approximation error present in the implementation of $\mathcal{C}1$ and $\mathcal{C}2$. We can improve the success probability when we have multiple copies of $\mathcal{C}$.

3.2 Approximating an unitary operation

Suppose U and V are two unitary operators on the same state space. We want to implement the operation of the operator U but instead of implementing U, we are able to implement the operator V. Operator V is called as an approximate implementation of the operator U. Let $E(U, V)$ denote the error when V is implemented instead of U. This error $E(U, V)$ is known as approximation error and is defined as:

$$E(U, V) = \max_{|\alpha\rangle} ||(U - V)|\alpha\rangle|| \tag{3.1}$$

Here, maximum is taken over all quantum states $|\alpha\rangle$ belonging to the same state space as U and V. Intuitively, if the operator V is applied on some input sate $|\chi\rangle$ instead of the operator U and the error $E(U, V)$ is small then any measurement applied on the state $V|\chi\rangle$ gives almost similar statistics which are obtained when measurement is applied on the state $U|\chi\rangle$. This intuition is formally described in lemma 5. The approximation result of the lemma is extremely useful and this result has also been found in book by Nielsen and Chuang[13].

Lemma 5. *Given two unitary operators U and V, let $E(U, V)$ denote the approximation error when V is implemented instead of U. Consider any state $|\psi\rangle$. Apply either of the*

operator U or V followed by the measurement of the state using any measurement operator say M. Let p_0 (or p_1) be the probability of getting a particular outcome when state $U|\psi\rangle$ (or $V|\psi\rangle$) is measured using M then $|p_0 - p_1| \leq 2E(U,V)$.

3.3 Problem statement

We introduced the approximate operator identification problem informally. In this section, we define the problem formally.

Definition 3 (**Approximate Operator Identification Problem**). *Given an operator $\mathcal{U}$ as a black-box which implements either operator U_1 or U_2, where U_1 and U_2 are arbitrary unitary operators. We are able to only approximate the unitary operators U_1 and U_2. Let V_1 (or V_2) be the approximate implementation of U_1 (or U_2) such that $E(U_1, V_1) \leq \epsilon_1$ and $E(U_2, V_2) \leq \epsilon_2$, where $\epsilon_1, \epsilon_2 \in \mathbb{R}$ and $0 < \epsilon_1, \epsilon_2 < 1$. The goal is to determine whether an unknown operator $\mathcal{U}$ is U_1 or U_2.*

3.4 Approximate Operator Identification

This section describes our approach to solve the approximate operator identification problem. The following steps will be followed to :

Step 1: Generate a quantum state $|\phi\rangle$ that is determined by the given operators V_1 and V_2 such that distance between $|\psi_1\rangle = V_1|\phi\rangle$ and $|\psi_2\rangle = V_2|\phi\rangle$ is maximal. The procedure of how to generate the initial state has been explained in the subsection 3.4.1. The metric used to compute the distance between the states and the reason of why we are trying to maximize the distance has also been shown in the subsection 3.4.1.

Step 2: Apply $\mathcal{U}$ to $|\phi\rangle$, where $\mathcal{U}$ is the unknown unitary operator given as black-box.

Step 3: Create two outcome measurement operator P such that, P can guess states $|\psi_1\rangle$ and $|\psi_2\rangle$ with minimal probability of failure. The procedure of how to create the measurement operator is explained shortly in the subsection 3.4.2.

Step 4: Measure the state $\mathcal{U}|\phi\rangle$ using P. Guess whether operator $\mathcal{U}$ is U_1 or U_2 according to the outcome of the measurement. This point will become more clear when we explain the complete process in some detail.

The following subsections will explain how the initial quantum state is generated using given operators and how to create measurement operator which will be used to identify the given unknown operator U. Also, an analysis has been done on the lower bound on the success probability of the proposed algorithm.

3.4.1 Generate initial quantum state $|\phi\rangle$

Given two operators V_1 and V_2, the problem is to generate a quantum state $|\phi\rangle$ such that distance between $|\psi_1\rangle = V_1 |\phi\rangle$ and $|\psi_2\rangle = V_2 |\phi\rangle$ is maximal. Here, the metric used to measure the distance between two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ is the trace distance that is defined as $D(|\psi_1\rangle, |\psi_2\rangle) = \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}$. There are many well known techniques for solving this problem[3, 10]. In this section, one of the techniques to solve the problem has been presented. If $D(|\psi_1\rangle, |\psi_2\rangle) = d$, then given one of these states chosen randomly from the set $\{|\psi_1\rangle, |\psi_2\rangle\}$, any algorithm can guess the correct state i.e which state has been chosen with at most $(1 + d)/2$ probability[11].

Therefore, the goal is to maximize the trace distance for the maximal success probability. This optimization problem is represented as follows:

$$\max_{|\phi\rangle} \sqrt{1 - |\langle\phi|\ V_1^\dagger\ V_2\ |\phi\rangle|^2}$$

Note that the above maximization problem is same as the following minimization problem:-

$$\min_{|\phi\rangle} |\langle\phi|\ V_1^\dagger\ V_2\ |\phi\rangle|^2 \tag{3.2}$$

The optimization problem represented by the equation (3.2) is same as the optimization problem discussed in section 2.3 of chapter 2. The goal in both of the optimization problems is to find an initial input state $|\phi\rangle$ and minimize $|\langle\phi|\ V_1^\dagger\ V_2\ |\phi\rangle|$. We have already discussed the algorithm to generate such input state and the corresponding minimum value of the expression represented by equation (3.2).

3.4.2 Create measurement operator

There are many possible ways to answer the question of how to create two outcome measurement operator P such that, P can guess states $|\psi_1\rangle$ and $|\psi_2\rangle$ with the minimal probability of failure[3, 11]. In this section, we will explain one of the techniques to answer this problem. The idea used to create the measurement operator can be found in the work

done by D Bera [3]. Let $P = \{P^0, P^1\}$ be the two outcome measurement operator with outcome **0 and 1**, where outcome **0** denotes the state $|\psi_1\rangle$ and **1** denotes the state $|\psi_2\rangle$. Let $\{|b_1\rangle, |b_2\rangle\}$ be two orthogonal basis states and P^0 and P^1 be the projectors onto the states $|b_1\rangle$ and $|b_2\rangle$ respectively. This means, we perform measurement in basis defined by the orthonormal basis $\{|b_1\rangle, |b_2\rangle\}$. Depending on the outcome corresponding to the state $|b_1\rangle$ or $|b_2\rangle$, we will guess the state to be $|\psi_1\rangle$ or $|\psi_2\rangle$. Our goal is to minimize the probability of error, i.e, when the state is $|\psi_1\rangle$ then we get an outcome corresponding to the basis $|b_2\rangle$ with the minimum probability. Similarly, we want the minimum error for the other state. We need to create orthonormal states $|b_1\rangle$ and $|b_2\rangle$ such that $|b_1\rangle$ is as close as possible to $|\psi_1\rangle$ and as far as possible from $|\psi_2\rangle$. In the same way, we need to have $|b_2\rangle$ close to $|\psi_2\rangle$. This implies $|\langle b_1|\psi_1\rangle|^2 = |\langle b_2|\psi_2\rangle|^2$.

The states $|\psi_1\rangle$ and $|\psi_2\rangle$ can be written in the form of $\{|b_1\rangle, |b_2\rangle\}$ basis for some $r_i, k_j \in \mathbb{R}$ (i = 1,2,3,4 and j = 1,2,3) as follows:

$$|\psi_1\rangle = r_1 \ |b_1\rangle + r_2 e^{\iota k_1} \ |b_2\rangle$$
$$|\psi_2\rangle = r_3 e^{\iota k_2} \ |b_1\rangle + r_4 e^{\iota k_3} \ |b_2\rangle$$

Let $\langle\psi_1|\psi_2\rangle = ke^{\iota k}$. We want $|\langle b_1|\psi_1\rangle|^2$ to be equal to $|\langle b_2|\psi_2\rangle|^2$. One possible solution is:

$$r_1 = r_4 = (\sqrt{1+k} + \sqrt{1-k})/2$$
$$r_2 = r_3 = (\sqrt{1+k} - \sqrt{1-k})/2$$
$$k_1 = 0, k_2 = k_3 = k$$

Then the required basis,

$$|b_1\rangle = \frac{1}{N}(-r_1 |\psi_1\rangle + r_2 e^{-\iota k} |\psi_2\rangle)$$
$$|b_2\rangle = \frac{1}{N}(r_2 |\psi_1\rangle - r_1 e^{-\iota k} |\psi_2\rangle)$$
$$Here, N = {r_2}^2 - {r_1}^2$$

Therefore we create the measurement operator P = $\{P^0, P^1\}$, where $P^0 = |b_1\rangle\langle b_1|$ and $P^1 = |b_2\rangle\langle b_2|$ with outcome **0** and **1**. The algorithm that follows the explained procedure

and creates the measurement operator is shown below (Algorithm 3). If the outcome is **0** then the state is guessed to be $|\psi_1\rangle$ i.e. operator is V_1 and outcome **1** guesses that state is $|\psi_2\rangle$ i.e. operator is V_2.

Algorithm 3: Algorithm to create measurement operator

input : State $|\psi_1\rangle$, $|\psi_2\rangle$
output: Measurement operator P = $\{P^0, P^1\}$

k $\leftarrow |\langle\psi_1|\psi_2\rangle|$
$r_1 \leftarrow (\sqrt{1+k}+\sqrt{1-k})/2$
$r_2 \leftarrow (\sqrt{1+k}-\sqrt{1-k})/2$
$N \leftarrow {r_2}^2 - {r_1}^2$
$|b_1\rangle \leftarrow \frac{1}{N}(-r_1|\psi_1\rangle + r_2 e^{-\iota k}|\psi_2\rangle)$
$|b_2\rangle \leftarrow \frac{1}{N}(r_2|\psi_1\rangle - r_1 e^{-\iota k}|\psi_2\rangle)$
$P^0 \leftarrow |b_1\rangle\langle b_1|$
$P^1 \leftarrow |b_2\rangle\langle b_2|$
return P = $\{P^0, P^1\}$

3.4.3 Analysis

For the analysis on the lower bound of the success probability of the proposed algorithm, we will consider both the cases: when $\mathcal{U} = U_1$ and $\mathcal{U} = U_2$. The lower bound will be computed for both the cases and the minimum of two bounds will give the final result.

Case 1. If $\mathcal{U} = U_1$ then

The probability of getting outcome **0** corresponding to the basis $|b_1\rangle$ when $|\psi_1\rangle = r_1\ |b_1\rangle + r_2 e^{\iota k_1}\ |b_2\rangle$ is measured is ${r_1}^2 = (1+\sqrt{1-k^2})/2$ (say p_0). But we have state $\overline{|\psi_1\rangle} = U_1|\phi\rangle$. Let p_1 be the probability of getting outcome **0** when $\overline{|\psi_1\rangle}$ is measured and we know that $E(U_1, V_1) \leq \epsilon_1$. Hence by lemma 5,

$$|p_0 - p_1| \leq 2\epsilon_1$$

Two possibilities are there. First if $p_1 \geq p_0$ and $p_0 = (1+\sqrt{1-k^2})/2$ then the probability of success is at least $(1+\sqrt{1-k^2})/2$. Second, if $p_1 < p_0$ then $p_1 \geq p_0 - 2\epsilon_1$ then the probability of success is at least $(1+\sqrt{1-k^2})/2 - 2\epsilon_1$. Therefore, the probability of success is at least $\min((1+\sqrt{1-k^2})/2, (1+\sqrt{1-k^2})/2 - 2\epsilon_1) = (1+\sqrt{1-k^2})/2 - 2\epsilon_1$.

Case 2. If $\mathcal{U} = U_2$ then

The probability of getting outcome **1** corresponding to the basis $|b_2\rangle$ when $|\psi_2\rangle = r_3 e^{\iota k_2}\ |b_1\rangle + r_4 e^{\iota k_3}\ |b_2\rangle$ is measured is ${r_4}^2 = (1+\sqrt{1-k^2})/2$. Similar to the case 1, the actual state

$\overline{|\psi_2\rangle} = U_2 |\phi\rangle$ and we know that $E(U_2, V_2) \leq \epsilon_2$. Similar analysis leads the following result: the probability of success i.e the probability of guessing the unknown operator is U_2 in this case is at least $\min((1+\sqrt{1-k^2})/2, (1+\sqrt{1-k^2})/2 - 2\epsilon_2) = (1+\sqrt{1-k^2})/2 - 2\epsilon_2$.

The proposed algorithm can solve the approximate Operator Identification Problem with at least $(1+\sqrt{1-k^2})/2 - 2.max(\epsilon_1, \epsilon_2)$ probability of success, where $k = \min_{|\phi\rangle} |\langle\phi| V_1^\dagger V_2 |\phi\rangle|^2$. Theorem 4 follows immediately:

Theorem 4. *Given an operator $\mathcal{U}$ as a black-box which implements either an arbitrary unknown unitary operator U_1 or U_2. Also given unitary operators V_1 and V_2 such that $E(U_1, V_1) \leq \epsilon_1$ and $E(U_2, V_2) \leq \epsilon_2$. There exists an algorithm that can guess whether $\mathcal{U}$ is U_1 or U_2 with the success probability of at least $(1+\sqrt{1-k^2})/2 - 2\epsilon$, where $k = \min_{|\phi\rangle} |\langle\phi| V_1^\dagger V_2 |\phi\rangle|^2$ and $\epsilon = max(\epsilon_1, \epsilon_2)$*

To summarize, even if we don't have an exact implementation of unitary operators that are possible candidates for a given unknown operator, we have an algorithm that can still guess the operation of the unknown operator with some success probability that depends on the implementation error.

Chapter 4

Multiple Operator Identification

In the previous two chapters, we discussed two different versions of the operator identification problem and designed an efficient algorithm to solve each of them. In this chapter, we will try to solve the generalized operator identification problem in which the candidate set size can be of any arbitrary size.

As a rough outline of this chapter, we begin with the problem statement and the application of the problem in the fault detection. In the following section, the algorithm to solve the problem has been proposed. Finally, an analysis of the proposed algorithm has been done.

4.1 Introduction

To recall, the operator identification problem is defined as: Given an operator $\mathcal{C}$ as a black-box which implements either operator $\mathcal{C}1$ or $\mathcal{C}2$ and $\mathcal{C}1 \neq e^{i\alpha}\mathcal{C}2$ for any α, the goal is to determine whether $\mathcal{C} = \mathcal{C}1$ or $\mathcal{C} = \mathcal{C}2$. In the first version of this problem, the exact implementation of the operation of $\mathcal{C}1$ and $\mathcal{C}2$ were known to us and we designed an efficient algorithm that was able to identify the operator with certainty. In chapter 3, the problem was modified such that only the approximate implementation of the operations of $\mathcal{C}1$ and $\mathcal{C}2$ were known to us. The algorithm was proposed that solved this modified problem with some probability. In both of the problems, the candidate set was considered to be of size two. In this chapter, we will consider the case when candidate set is of any size in general, say n. Thus, the operator identification problem can be formulated in general as follows: Given an operator $\mathcal{C}$ as a black-box and it is guaranteed that $\mathcal{C}$ implements one of the operators present in the candidate set $\{\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_n\}$. The goal is to determine which operator out of $\{\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_n\}$ is being implemented by the given

unknown $\mathcal{C}$. We call this modified operation identification problem as multiple operator identification problem.

To the best of our knowledge, no work has been done on how to extend the operator identification problem having candidate size of size two to the operator identification problem for candidate size of any size in general. Also, we believe that this is the first work that shows the approach to solve the multiple operator identification problem. In this chapter, an algorithm has been presented that solves this problem. The analysis of the probability of success and the results obtained is not that good, but the proposed idea can be used in the future related works to produce the efficient algorithm with better accuracy.

The general multiple operator identification problem defined above is important for detecting fault in a given circuit. Suppose, a circuit A is given that is constructed using m gates. For simplicity, consider the case when at some point of time, only one gate is faulty. The goal is to find which gate is faulty in the circuit. Let G_1, G_2, ..., G_m denote the gates present in the circuit A, when enumerated in the standard left to right manner. Let A_i denote the behaviour of the circuit when G_i gate is faulty and A_0 denote the case when none of the gates is faulty in the circuit. This problem of fault detection can be formulated in terms of multiple operator identification problem as follows: Consider the given circuit A as a black-box and the behaviour of A is implemented by one of the operation present in the candidate set $\{A_0, A_1, ..., A_m\}$. The goal is to determine the operation of A which will tell about the faulty gate.

4.2 Problem statement

In the previous section, we introduced the multiple operator identification problem informally. We also showed one application where multiple operator identification can be applied. In this section, we define the problem formally.

Definition 4 (**Multiple Operator Identification Problem**). *Given an operator $\mathcal{C}$ as a black-box and it is guaranteed that $\mathcal{C}$ implements one of the operators present in the candidate set $\{\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_n\}$, where $\mathcal{C}_i\{i = 1, 2, ..., n\}$ are arbitrary unknown unitary operators and $\mathcal{C}_i = e^{\iota\theta}\mathcal{C}_j$ for $i \neq j$. The goal is to determine which operator out of $\{\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_n\}$ is being implemented by the given unknown $\mathcal{C}$.*

4.3 Multiple Operator Identification

In this section, an approach to solve the problem of multiple operator identification has been proposed. Recall in the previous chapter, we used a distance metric named as approximation error that showed the similarity between the operators. If the distance between two operators say U and V is small then any measurement applied on the state $V|\chi\rangle$ gives almost similar statistics which are obtained when measurement is applied on the state $U|\chi\rangle$ for some input state $|\chi\rangle$. This same intuition has been used to solve the multiple operator identification problem. Our approach to solve the problem is as follows:

Step 1: Group the candidates present in the set $\{\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_n\}$ into two clusters. The complete procedure of how to cluster the elements of the set is explained shortly in the subsection 4.3.1.

Step 2: Once the clusters have been formed, find the center operator for both the clusters. The center operator will be one of the operators present in the candidate set. In subsection 4.3.2, the meaning of the center operator of the cluster has been explained and the procedure to find it has been shown. Let $\mathcal{C}_k$ and $\mathcal{C}_l$ be the center operators for both the clusters which were formed in Step 1.

Step 3: Generate a quantum state $|\phi\rangle$ that is determined by the given operators $\mathcal{C}_k$ and $\mathcal{C}_l$ such that distance between $|\psi_1\rangle = \mathcal{C}_k|\phi\rangle$ and $|\psi_2\rangle = \mathcal{C}_l|\phi\rangle$ is maximal.

Step 4: Apply $\mathcal{C}$ to the generated quantum state $|\phi\rangle$, where $\mathcal{C}$ is the unknown unitary operator given as black-box.

Step 5: Create two outcome measurement operator P such that P can guess states $|\psi_1\rangle$ and $|\psi_2\rangle$ with minimal probability of failure.

Step 6: Measure the state $\mathcal{C}|\phi\rangle$ using P. If the outcome of the operator P suggests that the operator that is being implemented by $\mathcal{C}$ is $\mathcal{C}_k$, then remove all the operators present in the cluster represented by the center operator $\mathcal{C}_l$ and vice versa.

Step 7: After removing one cluster, check the size of the remaining cluster. If the size of the remainder cluster is one, return the center operator of that cluster. Otherwise repeat steps 1-6 with the updated candidate set.

The following subsections will explain how to cluster the operators present in the candidate set and find the center operator of the cluster as required in steps 1 and 2 respectively. The procedure of how to generate the initial quantum state using given operators mentioned in step 3 and how to create the measurement operator that is used to identify the given unknown operator as required in step 5 has already been explained in the previous chapter.

4.3.1 Clustering the operators

The distance metric that is used for clustering the elements is same as the one used in the last chapter. It is denoted by $D(U, V)$ between any two operator V and U and is defined as:

$$D(U, V) = \max_{|\alpha\rangle} ||(U - V)\,|\alpha\rangle\,|| \tag{4.1}$$

Here, maximum is taken over all quantum states $|\alpha\rangle$ belonging to the same state space as U and V. We will use modified 2-mean clustering algorithm. The two important steps of the clustering include the initialization step and the assignment step. In initialization step, the initial representatives for the clusters are chosen and then in assignment step, each operator is assigned to one of the cluster. These two steps are as follows:

Initialization:

The first step is to choose the two initial representatives for the both the clusters. We will choose two operators $\mathcal{C}_k$ and $\mathcal{C}_l$ such that $D(\mathcal{C}_k, \mathcal{C}_l) = \max_{i,j} D(\mathcal{C}_i, \mathcal{C}_j)$ for all $1 \leq i, j \leq n$. The operators $\mathcal{C}_k$ and $\mathcal{C}_l$ will be called as representatives of the clusters.

Assignment:

The second step is assignment of the remaining $n - 2$ operators to one of these clusters. Each operator is assigned to the cluster whose representative has the least distance from it i.e. for each remaining operator C_i if $D(C_l, C_i) \leq D(C_k, C_i)$, assign the operator C_i to the cluster represented by the operator C_l otherwise in other cluster i.e. the cluster represented by the operator C_k.

4.3.2 Center Operator of the cluster

After the clustering of the candidate set, as explained in above subsection, two clusters of the given n operators are obtained. The next step is to find the representative of both the clusters which will be known as the center operator of the cluster. Lets first understand

what is meant by the center operator of the cluster. The center operator of the cluster is the operator C_o where the greatest distance $D(C_0, C_i)$ to all other vertices C_i is minimal. Note that this definition of the center of the cluster is same as the center of a graph. The center of the graph is the vertex of minimum eccentricity that is, the vertex u whose greatest distance to other vertices v is minimal. We know many efficient algorithms to find the center of the graph [9]. The same algorithm can be applied to find the center operator of the cluster. Note that the center operator can be one of the operators present in the candidate set. Many center operators may be possible but we can consider any one of them. Once the center operator has been found for the cluster, we will say that the cluster is represented by the obtained center operator.

After first two steps, we have two clusters and their center operators say C_l and C_k. Now we use these two operators to find the initial input state and the measurement operator as mentioned in steps 3 and 5. The procedure to generate the input state and the measurement operator has already been explained in the previous chapter.

4.3.3 Analysis

For the analysis of the proposed algorithm, consider for any arbitrary iteration of the algorithm say j, what is the probability of choosing the correct cluster given that we chose the correct cluster in the previous iteration. Let C_{lj} and C_{kj} be the center operator of the clusters in the j^{th} iteration. Now, there are two possibilities: first is when the actual operator for an unknown operator $\mathcal{C}$ belongs to the cluster represented by C_{lj} and the other one is when the actual operator belongs to the cluster represented by C_{kj}.

Case 1. Unknown operator $\mathcal{C}$ belongs to cluster of C_{lj}

Recall from the last chapter if $D(\mathcal{C}, C_{lj})$ is small then we can use C_{lj} as an approximate implementation for $\mathcal{C}$. If this is the case, then any measurement applied on the state $\mathcal{C}\,|\chi\rangle$ gives almost similar statistics which are obtained when measurement is applied on the state $C_{lj}\,|\chi\rangle$ for some input state $|\chi\rangle$. Note that $D(\mathcal{C}, C_{lj}) < D(\mathcal{C}, C_{kj})$. As a result, we will guess the correct cluster i.e, the cluster in which $\mathcal{C}$ belongs with the high probability. The formal analysis is same as the one done in the last chapter. We can consider C_{lj} as an approximate implementation for $\mathcal{C}$. Let $D(\mathcal{C}, C_{lj}) = \epsilon_0$ then the probability of choosing the correct cluster is at least $(1 + \sqrt{1 - k^2})/2 - 2\epsilon_0$, where $k = \min_{|\phi\rangle} |\langle\phi|\ {C_{lj}}^{\dagger}\ C_{kj}\ |\phi\rangle\,|^2$.

In the worst case, $\mathcal{C}$ will be at the farthest distance from the C_{lj} because of which the value of ϵ_0 will be maximum. But since we have chosen C_{lj} as the center operator so this will not matter much. For the worst case, $\epsilon_0 = \max_i \mathcal{C}_i$ for all $\mathcal{C}_i$ belonging to the cluster represented by C_{lj}. If the unknown operator $\mathcal{C}$ belongs to cluster represented by C_{lj} at some iteration and C_{lj} and C_{kj} are the center operators for the cluster at that iteration then the probability of choosing the correct cluster at that iteration given that we guessed the correct cluster in the previous iteration is at least $(1 + \sqrt{1 - k^2})/2 - 2\epsilon_0$, where $k = \min_{|\phi\rangle} |\langle\phi|\ {C_{lj}}^{\dagger}\ C_{kj}\ |\phi\rangle\ |^2$ and $\epsilon_0 = \max_i \mathcal{C}_i$ for all $\mathcal{C}_i$ belonging to the cluster represented by C_{lj}.

Case 2. Unknown operator $\mathcal{C}$ belongs to cluster of C_{kj}

Similar to the previous case, the same result is obtained: If the unknown operator $\mathcal{C}$ belongs to cluster represented by C_{kj} at some iteration and C_{lj} and C_{kj} are the center operators for the cluster at that iteration then the probability of choosing the correct cluster at that iteration given that we guessed the correct cluster in the previous iteration is at least $(1 + \sqrt{1 - k^2})/2 - 2\epsilon_1$, where $k = \min_{|\phi\rangle} |\langle\phi|\ {C_{lj}}^{\dagger}\ C_{kj}\ |\phi\rangle\ |^2$ and $\epsilon_1 = \max_i \mathcal{C}_i$ for all $\mathcal{C}_i$ belonging to the cluster represented by C_{kj}.

To summarize, the general multiple operator identification problem can be solved using the clustering of the given candidate set and identifying the center operator of the obtained clusters. The idea can be extended to get the better results to solve this problem.

Chapter 5

Conclusion and Future Work

In summary of this study, we have tried to solve the problem of distinguishing of unitary operators. We have considered different modifications of this problem and proposed an efficient algorithm for each one of those modifications. First, we considered the problem of operator identification that is related to the problem of distinguishing two pure quantum states. Typically an operator identification problem is defined as follows: Given an unknown operator $\mathcal{U}$ as a black-box which implements either an operator $\mathcal{U}1$ or an operator $\mathcal{U}2$, where $\mathcal{U}1$ and $\mathcal{U}2$ are arbitrary unitary operators and their operation is known to us. The goal is to determine whether an unknown operator $\mathcal{U}$ is an implementation of $\mathcal{U}1$ or $\mathcal{U}2$. We proposed an efficient algorithm to solve the operator identification problem without any error. The proposed algorithm uses the tool known as amplitude amplification. Amplitude amplification is used to increase the success probability of a quantum algorithm.

In the above version of the problem, the operations of $\mathcal{U}1$ and $\mathcal{U}2$ are the arbitrary unitary operations. In quantum circuit theory, it is not always possible to implement any arbitrary operation exactly in an efficient way but it turns out that we can approximate the required unitary operations. As a result, we considered the modification in the above problem as : Given an operator $\mathcal{U}$ as a black-box which implements either operator $\mathcal{U}1$ or $\mathcal{U}2$, the aim is to guess whether $\mathcal{U}$ implemented $\mathcal{U}1$ or $\mathcal{U}2$. We don't have an exact implementation of $\mathcal{U}1$ and $\mathcal{U}2$ but we are only able to approximate the operations of $\mathcal{U}1$ and $\mathcal{U}2$. We proposed an efficient algorithm to solve this problem. The proposed algorithm uses only one query to the black-box $\mathcal{C}$ to guess whether $\mathcal{C} = \mathcal{C}1$ or, $\mathcal{C} = \mathcal{C}2$ with some probability. We also find the lower bound on the success probability and show how it depends on the approximation error present in the implementation of $\mathcal{C}1$ and $\mathcal{C}2$.

We can improve the success probability when we have multiple copies of $\mathcal{C}$.

Finally we consider the general version of this problem: Given an operator $\mathcal{U}$ as a black-box and it is guaranteed that $\mathcal{U}$ implements one of the operators present in the candidate set $\{\mathcal{U}_1, \mathcal{U}_2, ..., \mathcal{U}_n\}$. The goal is to determine which operator out of $\{\mathcal{U}_1, \mathcal{U}_2, ..., \mathcal{U}_n\}$ is being implemented by the given unknown $\mathcal{U}$. We proposed an algorithm to solve this problem. The proposed algorithm clusters the candidate set into 2-cluster and guess the correct cluster with some probability in which unknown operator $\mathcal{U}$ falls. It then removes other cluster from the candidate set. The steps of the algorithm are repeated until one operator is left.

The analysis and result of this general version of the problem is not that good but the proposed idea can be used in the future to produce an efficient algorithm for the problem. For better analysis and result we may use different metric to measure the distance between the operators.

Bibliography

[1] Antonio Acin. Statistical distinguishability between unitary operations. Physical review letters, 87(17):177901, 2001.

[2] Koenraad MR Audenaert, John Calsamiglia, Ramón Munoz-Tapia, Emilio Bagan, Ll Masanes, Antonio Acin, and Frank Verstraete. Discriminating states: The quantum chernoff bound. Physical review letters, 98(16):160501, 2007.

[3] Debajyoti Bera. Detection and diagnosis of single faults in quantum circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 37(3):587–600, 2018.

[4] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. Contemporary Mathematics, 305:53–74, 2002.

[5] G Mauro D'Ariano, Paoloplacido Lo Presti, and Matteo GA Paris. Using entanglement improves the precision of quantum measurements. Physical review letters, 87(27):270404, 2001.

[6] Yuan Feng, Runyao Duan, and Mingsheng Ying. Unambiguous discrimination between mixed quantum states. Physical Review A, 70(1):012308, 2004.

[7] Ofer Grossman and Dana Moshkovitz. Amplification and derandomization without slowdown. In Foundations of Computer Science (FOCS), 2016 IEEE 57th Annual Symposium on, pages 770–779. IEEE, 2016.

[8] Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219. ACM, 1996.

[9] S Louis Hakimi. Optimum locations of switching centers and the absolute centers and medians of a graph. Operations research, 12(3):450–459, 1964.

[10] Akinori Kawachi, Kenichi Kawano, François Le Gall, and Suguru Tamaki. Quantum query complexity of unitary operator discrimination. In International Computing and Combinatorics Conference, pages 309–320. Springer, 2017.

[11] Phillip Kaye, Raymond Laflamme, Michele Mosca, et al. An introduction to quantum computing. Oxford University Press, 2007.

[12] Carlos Mochon. Family of generalized "pretty good" measurements and the minimal-error pure-state discrimination problems for which they are optimal. Physical Review A, 73(3):032328, 2006.

[13] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.