THE HIDDEN SUBGROUP PROBLEM

By

ANALES DEBHAUMIK

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

2010

I dedicate this to everyone who helped me in my research.

ACKNOWLEDGMENTS

First and foremost I would like to express my sincerest gratitude to my advisor Dr Alexandre Turull. Without his guidance and persistent help this thesis would not have been possible.

I would also like to thank sincerely my committee members for their help and constant encouragement.

Finally I would like to thank my wife Manisha Brahmachary for her love and constant support.

TABLE OF CONTENTS

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

THE HIDDEN SUBGROUP PROBLEM

By

Anales Debhaumik

May 2010

Chair: Alexandre Turull
Major: Mathematics

The topic of my research is the *Hidden Subgroup Problem*. The problem can be stated as follows:

Problem. *(Hidden Subgroup Problem) Let G be a finite group and H a subgroup. Given a black-box function $f : G \to S$ which is constant on (left)-cosets gH of H and takes different values for different cosets, determine a set of generators for H.*

Efficient classical algorithms for the Hidden Subgroup Problem are not known. However, efficient quantum algorithms are known for this problem in some cases. One such algorithm implies Shor's famous efficient method for breaking the RSA cryptosystem.

An efficient solution of this problem in all cases would have wide implications in the field of theoretical computer science. For example it would most likely solve some classical problems which are neither **NP**−complete nor are in **P**. A solution would also imply a solution for Graph Isomorphism problem which is a long standing problem in computer science.

In the present thesis, we study some quantum algorithms for the *Hidden Subgroup Problem*. We discuss Quantum Fourier Tranform and its applications to the Hidden Subgroup Problem. We discuss Almost Abelian groups and show that there is a quantum algorithm that solves the Hidden Subgroup Problem for them. We also study the decision version of the problem. We compare two different formalizations of

this concept. We show that these formalizations coincide in the case of abelian and Frobenius groups. We conclude with a family of groups where the formalizations may not coincide.

CHAPTER 1
INTRODUCTION

1.1 Preliminaries

A quantum computer is an, at present theoretical, machine which performs computations on the basis of the laws of quantum mechanics. Such a device can prepare quantum states and perform measurements on them. As with classical computers, numerical data form the input and the output for the quantum computer. The processing of this data in a quantum computer may involve actions on them which are not classical. As a result, the output of a quantum computer is not fully determined by its input. Given a particular input, various outputs may occur with different probabilities. In this sense, quantum computers behave differently than classical ones.

Though quantum computing as a field of research is still in its infancy significant amount of work has already been done in this field. In 1985 Deutsch gave a quantum algorithm for a very simple problem and showed that it worked better than a classical one. In his problem we are given a blackbox which computes a simple function. The box takes two bits as input and outputs two bits. It implements one of the four following functions from $\mathbb{F}_2^2 \to \mathbb{F}_2^2$:

$f_1(x, y) = (x, y)$

$f_2(x, y) = (x, y + 1)$

$f_3(x, y) = (x, x + y)$

$f_4(x, y) = (x, x + y + 1)$

The goal is to determine whether the function implemented by the box is in the set $\{f_1, f_2\}$ or $\{f_3, f_4\}$. On a classical computer it will take 2 queries to find the answer to the question. But on a quantum computer it will take just 1 query to find the answer. In 1992 Deutsch and Jozsa (7) gave the first non-trivial quantum algorithm. Their problem is the generalization of the above problem. In this problem we are given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The goal is to find out how many queries to the box are needed in the

worst case to determine whether the function is a constant or balanced (0 on one half of the domain states and 1 on the other half). For the classical case the problem has exponential query complexity. But for the quantum case as was shown by Deutsch and Jozsa only a single query is needed. Motivated by this Berstein and Vazirani (3) gave a quantum algorithm which worked significantly faster (super-polynomial speedup) than the best classical algorithm. The Berstein Vazirani problem has a non-recursive and a recursive version. In the non-recursive version we are given a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. The function is $f_s(x) = x.s$ for some unknown s where $x.s$ denotes the dot product. The goal is to find s. In the classical case the query complexity is at least n whereas for the quantum case only a single query is needed. The recursive version is a little more complex than the non-recursive one. Simon (24) then gave a quantum algorithm which performed exponentially faster than its classical counterpart. In Simon's problem we are given an integer $m \geq 1$ and a function $f : \mathbb{F}_2^m \rightarrow R$, where R is a finite set. We also know that there exists a nonzero element $s \in \mathbb{F}_2^m$ such that for all $x, y \in \mathbb{F}_2^m$ $f(x) = f(y)$ if and only if x=y or $x = y + s$. The goal is to find s. All these paved the way for Shor's celebrated paper on factoring and discrete log (23). There is no known efficient classical algorithm for factoring a large number n. The security and robustness of RSA public-key cryptosystem is based on this fact. Shor showed in his paper that given a quantum computer factoring of a number n can be done in polynomial time.

Simon's and Shor's algorithms laid the framework for a very important problem of quantum computation known as the Hidden Subgroup Problem. The problem can be stated as follows.

Problem. *(Hidden Subgroup Problem) Let G be a finite group and H a subgroup. Given a black-box function $f : G \rightarrow S$ which is constant on (left)-cosets gH of H and takes different values for different cosets, determine a set of generators for H.*

The Hidden Subgroup Problem is at the heart of Shor's and Simon's problems. In Shor's problem given n let a be any integer such gcd(a, n)=1. Let r be the order of

$a \in \mathbb{Z}_n^*$. The goal is to find r. In this problem G is $\mathbb{Z}$ and H is $r\mathbb{Z}$. For practical purposes we can work with $\mathbb{Z}_m$ where $m = 2^l > n$. The function f is given by $f(x) = a^x + n\mathbb{Z}$. Simon's problem reduces to a special case of the Hidden Subgroup Problem if we take G to be $\mathbb{F}_2^m$ and $H = \{0, s\}$.

Efficient quantum algorithms for The Hidden Subgroup Problem are known for abelian groups thanks to the efforts of Shor, Simon, Deutsch etc (7). The non-abelian case still poses a challenge. Some positive results have been obtained for Dihedral group by M. Ettinger and P. Hoyer (8), G. Kuperberg (19), Regev (21), Dave Bacon, Andrew M. Childs and Wim van Dam (1). Efficient quantum algorithms have been obtained for semidirect product of the forms $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$ by Yoshifumi Inui and Francois Le Gall (15), for $\mathbb{Z}_N \rtimes \mathbb{Z}_p$ where $N = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ and prime p does not divide $p_j - 1$ by Dong Pyo Chi, Jeong San Kim and Soojoon Lee (5), for some metacyclic groups and all groups of the form $\mathbb{Z}_p^r \rtimes \mathbb{Z}_p$ for any prime p and a fixed r by Dave Bacon, Andrew M. Childs and Wim van Dam (1), for Wreath product of the form $\mathbb{Z}_2^n \wr \mathbb{Z}_2$ by M. Rotteler and T. Beth (4), for some solvable groups by K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen (10) and for groups with small commutators by G. Ivanyos, F. Magniez, and M. Santha (17). Unfortunately a unified solution has still not been found.

An efficient solution of this problem would have wide implications in the field of theoretical computer science. For example it would most likely solve some classical problems which are neither **NP**−complete nor are in **P**. A solution would also imply a solution for Graph Isomorphism problem which is a long standing problem in computer science.

In this paper we study distinguishability of the Hidden Subgroup Problem for Frobenius groups of the forms $\mathbb{Z}_{\alpha(\beta)}^{g(\beta)} \rtimes \mathbb{Z}_\beta$, $\mathbb{Z}_\alpha^{g(i)} \rtimes \mathbb{Z}_{m(i)} \rtimes \mathbb{Z}_{n(i)}$, $\mathbb{Z}_\alpha^{g(i)} \rtimes (SL(2,5) \times (\mathbb{Z}_{m(i)} \rtimes \mathbb{Z}_{n(i)})$. For groups of the form $\mathbb{Z}_{\alpha(\beta)}^{g(\beta)} \rtimes \mathbb{Z}_\beta$ we give a necessary and sufficient condition for the distinguishability of the subgroups given that $g(\beta) > \beta^{\frac{1}{c}}$ for some $c > 0$ and for all sufficiently large β. We also give a necessary sufficient condition for the distinguishability

of the subgroups of Frobenius groups of the type $\mathbb{Z}_\alpha^{g(i)} \rtimes \mathbb{Z}_{m(i)} \rtimes \mathbb{Z}_{n(i)}$ given that $g(i)^c \geq m(i)n(i)$ for some $c > 0$ and sufficiently large i. Based on the condition that $g(i)^c \geq m(i)n(i)$ for some $c > 0$ and sufficiently large i we give a necessary and sufficient condition for the distinguishability of the subgroups of $\mathbb{Z}_\alpha^{g(i)} \rtimes (SL(2,5) \times (\mathbb{Z}_{m(i)} \rtimes \mathbb{Z}_{n(i)})$. In (11) M. Grigni, L. J. Schulman, M. Vazirani, U. Vazirani gave an efficient algorithm for "almost abelian groups." They also give an outline of how the algorithm works for "almost abelian groups" $\mathbb{Z}_3 \rtimes \mathbb{Z}_m$ where m is a power of 2. In section 7 we describe the algorithm for these groups and give an estimate of the number of steps required to obtain the hidden subgroups with probability bigger than $\frac{1}{2}$.

1.2 Quantum Computing

The theory of quantum computing was launched in the beginning of 1980. The famous physicist Feynman in an article (9) proposed that it is not possible to simulate a quantum system on a classical computer without exponential slowdown. He also suggested that a quantum computer could be a way to avoid such slowdown. In 1985 Deutsch (6) first gave a description of a universal quantum computer which was refined later by some other computer scientists. Though a quantum computer is still out of reach a lot of theoretical progress has been made ever since.

To understand a quantum computer we first have to know a few things about quantum mechanics and quantum system. In quantum mechanics a state in an n-level system is a unit vector in an n dimensional complex vector space H_n with an orthonormal basis chosen as $|x_1\rangle, |x_2\rangle, ..., |x_n\rangle$. The choice of such a basis is arbitrary. Any state in a quantum system can thus be written as $p_1|x_1\rangle + p_2|x_2\rangle + ... + p_n|x_n\rangle$ where the $p_i \in \mathbb{C}$ are called the amplitudes (13) with the requirement that $\sum_{i=1}^{n} |p_i|^2 = 1$ The amplitudes signify that the probability that a property x_i is observed of the system is $|p_i|^2$. The linear combinations of the basis states are called *superposition of states*.

The basic unit of information for a classical computer is a bit. Similarly a quantum computer operates on quantum bits known as *qubits*. It is basically a 2-level quantum

system and can be identified with a 2-dimensional Hilbert space with basis $|0\rangle, |1\rangle$. A general state of a quantum system is thus equal to $c_1|0\rangle + c_2|1\rangle$ where the c_i are complex numbers and $|c_1|^2 + |c_2|^2 = 1$.

If we have two systems with basis states $|x_1\rangle, |x_2\rangle, ..., |x_n\rangle$ and $|y_1\rangle, |y_2\rangle, ..., |y_m\rangle$ then the compound system will have basis states as ($|x_i\rangle, |y_i\rangle$). Thus a system of two qubits is a 4-dimensional Hilbert space with an orthonormal basis $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$. A quantum register of length m is an ordered system of m qubits associated with the 2^m-dimensional space $H_2 \bigotimes H_2 .... \bigotimes H_2$.

An operation on m qubits can be represented by a unitary map $U : H \rightarrow H$ where H is a 2^m-dimensional Hilbert space representing the quantum system. It can also be represented by a unitary matrix. As a very simple example we can consider the not operation on a single qubit. The operation takes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. The matrix that defines this operation is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The process of getting information out of a quantum state is known as measurement. There are several ways to think about measurement. The simplest one is measurement in the computational basis. Suppose we are in a quantum system with n-dimensional basis vectors and $|\alpha\rangle = \sum_0^{n-1} p_j|j\rangle$ is a quantum state. Measurement in the computational basis will return the state $|j\rangle$ with probability $|p_j|^2$ and after the measurement the output state becomes $|\alpha'\rangle = |j\rangle$. Thus the given state collapses to the one returned by the measurement and all other information about the state is destroyed.

1.3 Quantum Fourier Transform

One reason why a quantum computer can work more efficiently than a classical one, as demonstrated by the performances of the efficient quantum algorithms, is that quantum fourier transform can be implemented on it. It is the key ingredient for some very interesting quantum algorithms. It also accounts for the efficiency of the period

finding algorithms like the ones devised for various instances of the Hidden Subgroup Problem.

Let G be a finite group of order n and let $R = \{\rho^1, \rho^2, ..., \rho^\nu\}$ be a complete set of inequivalent complex irreducible representations of G with degrees d_{ρ_i} $i = 1, ..., \nu$. We choose these representations to be unitary ((16), *Theorem* 4.17). Let S_{time} be a complex vector space of dimension $|G|$ with an orthonormal basis $B_{time} = \{|g_1\rangle, |g_2\rangle, ..., |g_n\rangle\}$ where the g_i are the elements of the group G. Let S_{space} be another complex vector space with an orthonormal basis $B_{space} = \{|\rho^1, 1, 1\rangle, |\rho^1, 1, 2\rangle, ..|\rho^k, i, j\rangle, ..., |\rho^\nu, d_{\rho^\nu}, d_{\rho^\nu}\rangle\}$ formed by considering the $(i, j)th$ entry of the matrix $\rho(g)$ for each $\rho \in R$ and $g \in G$. Since there are d_ρ^2 matrix entries in the matrix $\rho(g)$ for each $\rho \in R$, there are $\sum_{i=1}^{\nu} d_{\rho^i}^2 = |G|$ number of basis vectors. So the dimension of S_{space} is $|G|$ which is the same as S_{time}.

We are now ready to define Quantum Fourier Transform.

Definition 1. QFT or quantum fourier transform over a group G is the linear map $Q_G : S_{time} \to S_{space}$ such that

$$Q_G(|g\rangle) = \frac{1}{\sqrt{|G|}} \sum_{\rho,i,j} \sqrt{d_\rho}\rho(g)_{i,j}|\rho, i, j\rangle$$

where $\rho \in R$ has dimension d_ρ, and $\rho(g)_{i,j}$ is the (i, j)th entry of the matrix $\rho(g)$ for $g \in G$ and $1 \leq i, j \leq d_\rho$

We will now show that the QFT is a unitary transformation.

Let $g_p, g_q \in G$. Then, since the basis S_{space} is orthonormal, we have

$$\langle Q_G(|g_p\rangle), Q_G(|g_q\rangle)\rangle = \frac{1}{|G|} \sum_{\rho,i,j} d_\rho \rho(g_p)_{i,j} \overline{\rho(g_q)_{i,j}} \langle|\rho, i, j\rangle, |\rho, i, j\rangle\rangle.$$

Since ρ is unitary, $\overline{\rho(g)_{ij}} = \rho(g^{-1})_{ji}$ and the previous expression becomes

$$\frac{1}{|G|} \sum_{\rho,i,j} d_\rho \rho(g_p)_{i,j} \rho(g_q^{-1})_{j,i} = \frac{1}{|G|} \sum_{\rho} d_\rho \chi_\rho(g_p g_q^{-1})$$

where χ_ρ is character afforded by ρ. By the second orthogonality relation ((16), *Theorem* 2.18)

$$\frac{1}{|G|}\sum_{\rho} d_\rho \chi_\rho(g_p g_q^{-1}) = \begin{cases} 1 & \text{for } p = q \\ 0 & \text{otherwise} \end{cases}$$

So we have shown that $\langle |g_p\rangle, |g_q\rangle\rangle = \langle Q_G(|g_p\rangle), Q_G(|g_q\rangle)\rangle$. Hence QFT is unitary.

Quantum Fourier Transform is an extremely powerful tool which has been used to devise efficient quantum algorithms for the Hidden Subgroup Problem. QFT runs in polynomial time for abelian groups and this fact has been exploited to find an efficient general algorithm for the abelian HSP. Extensive research is being done to find efficient QFT in the case of non-abelian groups. Zalka (25) gives an efficient HSP algorithm for wreath product groups of the form $G = \mathbb{Z}_2^n \wr \mathbb{Z}_2$ where he computes QFT efficiently for the group. Peter Hoyer (14) gives construction of QFT for Quaternions and some Metacyclic groups. Beth, Puschel, Rotteler, (4) show how to do QFT efficiently on a class of groups - solvable 2 groups containing a cyclic normal subgroup of index 2. Beals (2) shows how to compute QFT over S_n in time $\bigcirc(poly(n))$. Christopher Moore, Daniel Rockmore, Alexander Russell (20) give efficient QFT-that is circuits of poly($\log(|G|)$) size-for groups like the Clifford group, symmetric group, metabelian groups including metacyclic groups such as the dihedral and affine groups.

1.4 Hidden Subgroup Problem

In this paper we focus on the Hidden Subgroup Problem. There are two versions of the problem.

Hidden Subgroup Problem: Let G be a finite group and H a subgroup. Given a black-box function $f : G \to S$ which is constant on (left)-cosets gH of H and takes different values for different cosets, determine a set of generators for H.

An algorithm is a procedure to solve a computational problem. A classical algorithm is one which performs a finite number of steps and outputs the answer to the problem. Since the behavior of a quantum computer is not fully determined by its input, the

outcome of a quantum algorithm is necessarily uncertain, but we may calculate the probability that it produces the correct answer to the problem. We say that a quantum algorithm solves the problem if for every input it returns the correct answer to the problem after a finite number of steps with probability p, for some $p > \frac{1}{2}$. Even though an algorithm performs a finite number of steps it may run for a long time depending on the inputs.

It is believed that a good way to estimate the running time of any algorithm to solve the Hidden Subgroup Problems is to count the number of queries made to the black box function. The complexity of the problems is estimated by $|G|$. We say that an algorithm for a class of problems is *efficient* if there is some polynomial $p(x) \in \mathbb{R}[x]$ such that the number of queries to the black box function required by the algorithm is always at most $p(\log |G|)$.

An obvious algorithm to solve the Hidden Subgroup Problem would be to evaluate $f(g)$ for all $g \in G$, and to notice that $H = \{g \in G : f(g) = f(1)\}$. This requires $|G|$ queries to the function f and so this algorithm is not efficient. More efficient quantum algorithms have been obtained involving Quantum Fourier Sampling.

Quantum Fourier sampling is a method which can be implemented by a quantum computer to produce with a single query to the black box function an irreducible representation ρ of G which has $core_G(H)$ in its kernel where $core_G(H)$ is the largest subgroup of H normal in G. If ρ affords the character χ_ρ then the probability of Quantum Fourier sampling yielding ρ is $P_H(\rho) = \frac{d_\rho |H|}{|G|} \langle (\chi_\rho)_H, 1_H \rangle$, where $\langle (\chi_\rho)_H, 1_H \rangle = \frac{1}{|H|} \sum_{h \in H} \chi_\rho(h)$.

Quantum Fourier sampling can be implemented on a quantum computer as follows. The setup is almost the same as in the previous section. We have S_{time} with basis B_{time} indexed by the elements g_i $1 \leq i \leq n$ of the group G. Fourier Transform Q_G sends S_{time} to S_{space} which is another complex vector space with basis B_{space}. Let us define a complex vector space S_M with orthonormal basis $\{|g_1, s_1\rangle, |g_1, s_2\rangle, ..., |g_n, s_n\rangle\}$ where

$g_i \in G$ and $s_i \in \{0\} \bigcup S$. We also define a unitary map $Q_f : S_{time} \rightarrow S_M$ given by $Q_f(|g\rangle) = |g, f(g)\rangle$. The method of Fourier Sampling is now detailed below:

Step 1 : First prepare a state in S_M as below.

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, 0\rangle$$

Step 2 : Compute Q_f defined on S_{time} and get the state

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, f(g)\rangle.$$

which is in S_M.

Step 3 : Measure the second register. If the measured value is f_m we get the state

$$|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch, f_m\rangle \in S_M.$$

Now for each $f_m \in S$, S_{time} is isomorphic to the subspace of S_M with basis $\{|g_1, f_m\rangle, |g_2, f_m\rangle, ..., |g_n, f_m\rangle\}$. Hence $|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch, f_m\rangle$ can be identified with the state $|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle$.

Step 4 : QFT is performed over the state $|cH\rangle$ which yields

$$\frac{1}{\sqrt{|G||H|}} \sum_{\rho, i, j} \sqrt{d_\rho} \sum_{h \in H} \rho_{ij}(ch) |\rho, i, j\rangle.$$

Step 5 : Measure ρ.

The probability to observe any particular ρ under Quantum Fourier sampling is

$$P_H(\rho) = \sum_{i,j} \frac{d_\rho}{|G||H|} |\sum_{h \in H} \rho_{ij}(ch)|^2.$$

For an $n \times n$ matrix M we let $\|M\|$ denote the matrix norm given by

$$\|M\|^2 = trace(M^* M) = \sum_{i,j} |M_{ij}|^2$$

where, for any matrix M, M^* denotes the transpose of its complex conjugate. Then

$$P_H(\rho) = \frac{d_\rho}{|G||H|} \| \sum_{h \in H} \rho(ch) \|^2.$$

Now

$$\|\sum_{h\in H}\rho(ch)\|^2 = trace((\sum_{h\in H}\rho(ch))^*\sum_{h\in H}\rho(ch)) =$$

$$trace((\sum_{h\in H}\rho(h))^*\rho(c)^*\rho(c)\sum_{h\in H}\rho(h)) = \|\sum_{h\in H}\rho(h)\|^2$$

since $\rho(c)$ is unitary. Hence

$$P_H(\rho) = \frac{d_\rho|H|}{|G|}\|\frac{1}{|H|}\sum_{h\in H}\rho(h)\|^2.$$

Now ρ_H is a representation of H not necessarily irreducible. It can, however, be decomposed into irreducible representations over H. With proper choice of basis we can make $\rho(h)$ block diagonal with each block corresponding to an irreducible representation η_t. If m =the number of conjugacy classes of H then $1 \leq t \leq m$. Hence each diagonal entry of $\sum_{h\in H}\rho(h)$ is $\sum_{h\in H}\eta_t(h)$ for some $1 \leq t \leq m$. By ((22), *Corollary* 3 Chapter 2)

$$\sum_{h\in H}\eta_t(h) = \begin{cases} |H| & \text{for } \eta_t = 1_H \\ 0 & \text{otherwise} \end{cases}.$$

Hence we see that $\|\frac{1}{|H|}\sum_{h\in H}\rho(h)\|^2 = \langle(\chi_\rho)_H, 1_H\rangle$ where χ_ρ is the irreducible character afforded by ρ. Thus

$$P_H(\rho) = \frac{d_\rho|H|}{|G|}\langle(\chi_\rho)_H, 1_H\rangle.$$

A class of quantum algorithms to solve the Hidden Subgroup Problem using quantum Fourier Sampling have been developed. They are called the Weak Standard Method.

Weak Standard Method: Given the input of the Hidden Subgroup Problem, select some number $n = Q(\log|G|)$. Apply quantum Fourier sampling n times and obtain representations ρ_1, ρ_2,..., ρ_n. Output the subgroup $\bigcap_{i=1}^n ker(\rho_i)$.

It has been shown in (12) that $n = 4\log|G|$ is enough to retrieve $core_G(H)$ with probability bigger than $\frac{1}{2}$. If the hidden subgroup $H \trianglelefteq G$ then $core_G(H) = H$ and the Weak Standard Method outputs the hidden subgroup H with high probability.

There is another method which is believed to be more powerful than Weak Standard Method. It is known as the strong standard method. In the *Strong Standard Method* both ρ and its entries i, j are sampled. It is believed that in certain cases such sampling gives more information about H than the Weak Standard Method.

1.5 Distinguishability

There is a decision version of the Hidden Subgroup problem. It is stated as follows.

Decision Version of the Hidden Subgroup Problem : Let G be a finite group and H a subgroup. Given a black-box function $f : G \to S$ which is constant on (left)-cosets gH of H and takes different values for different cosets, determine whether $H = \{e\}$ or not.

Certain subgroups H of G may produce probabilities of representations under Quantum Fourier Sampling that are very close to those that arise from the trivial subgroup. In this case we would say that H is indistinguishable from the trivial subgroup. In 2005 Kempe and Shalev (18), proposed the following definition of indistinguishable subgroup.

Definition 2. Let G be a finite group. Let $\mathrm{Irr}(G)$ be the set of irreducible (complex) representations of G. We denote by χ_ρ the character associated to a $\rho \in \mathrm{Irr}(G)$ and let d_ρ be it's degree. For $H < G$ we define

$$\mathbf{D}_H = \frac{1}{\mid G \mid} \sum_{\rho \in \mathrm{Irr}(G)} d_\rho \mid \sum_{h \neq e, h \in H} \chi_\rho(h) \mid .$$

We say that a subgroup H is Kempe-Shalev distinguishable if $\mathbf{D}_H \geq log(\mid G \mid)^{-c}$ for some $c > 0$, c being independent of G.

Using this definition , Kempe and Shalev classified the distinguishable subgroups of S_n.

In chapter 3 we prove that all the non-trivial subgroups of an abelian group are Kempe-Shalev distinguishable. We also classify the Kempe-Shalev distinguishable subgroups of some Frobenius groups.

While the Kempe Shalev definition captures the difficulty of distinguishing the hidden subgroup from the trivial group in some cases, it is not always obvious how to translate its answers to practical algorithms. In chapter 4 we define ”Algorithmic distinguishability” which defines distinguishability of a subgroup H of any finite group G from the trivial one on the basis of when a natural algorithm that uses the weak standard method succeeds in polynomial time. We prove that the non-trivial subgroups of an abelian group are algorithmic distinguishable. We also show that the Kernels of the Frobenius groups, which are Kempe-Shalev distinguishable, are also algorithmic distinguishable and the complements, which are not Kempe-Shalev distinguishable, are also not algorithmic distinguishable.

Even though in case of Frobenius groups the two concepts seem to coincide, we show in chapter 5 that they might not be the same. Though we don't have a general proof, computations show that the two concepts may be different for $G = S_3 \times S_3 \ldots \times S_3 (n \ \ copies)$.

CHAPTER 2
HIDDEN SUBGROUPS FOR ALMOST ABELIAN GROUPS

In (11) the notion of an almost abelian group was introduced.

Definition 3. (Almost Abelian Group): Let G be a finite group. Let $N_G(H)$ denote the normalizer of a subgroup H in G. Consider the normal subgroup $K(G) = \bigcap_H N(H)$ of G. We call G almost abelian if $[G : K(G)] \in exp(\bigcirc(\lg^{\frac{1}{2}}(n)))$ where $n = \lg(|G|)$.

In (11) the authors give an algorithm to find the hidden subgroups of an almost abelian group. In this chapter we give a very small variation of their algorithm. We prove that this algorithm succeeds with a small number of iterations with probability greater than $1/2$ on every almost abelian group. We analyse in detail the outcomes of running this algorithm in the case of the group $G = \mathbb{Z}_3 \rtimes \mathbb{Z}_m$ where $m = 2^n$. and any non-trivial hidden subgroup. We find the probability that the process will yield any particular subgroup after i iterations.

2.1 Algorithm to find the hidden subgroups

The algorithm to determine the hidden subgroups for the almost abelian groups is as follows:

Repeat Weak Standard Method $n = s(\log|G|)$ times, where $s(x) \in \mathbb{R}[x]$ is a non-zero polynomial, for all the subgroups of G containing $K(G)$. Consider the intersections of the kernels of the representations observed in each case after n repetitions. The algorithm returns the largest such intersection.

The algorithm can be formally written as follows:

Step I: Repeat weak Standard Method $n = s(\log|G|)$ times, where $s(x) \in \mathbb{R}[x]$ is a nonzero polynomial for all subgroups of G containing $K(G)$.

Step II: Take the intersections of the kernels of the representations observed in each case after n repeats.

Step III: Return the largest such intersection.

Notice that this algorithm extends the Weak Standard Method to find any hidden subgroup and not just the normal ones. We now estimate the number of iterations needed so that the probability of retrieving the hidden subgroup is more than $1/2$.

Lemma 2.1. *Let G be a finite group of order a and H the hidden subgroup. Suppose for each subgroup M of G the probability of getting $core_M(H)$ be $1 - 2e^{-\frac{\lg(|K(G)|)}{k}}$. Then the product of these probabilities is greater than $1/2$ if $k < \frac{\lg|K(G)|}{\ln(4)+(\lg(a))^2}$.*

Proof.

$$(1 - 2e^{-\frac{\lg(|K(G)|)}{k}})^{2^{\lg^2 a}} > 1 - 2^{\lg^2 a}\frac{2}{e^{\frac{\lg|K(G)|}{k}}} > 1 - e^{\lg^2 a}\frac{2}{e^{\frac{\lg|K(G)|}{k}}} > 1/2$$

implies $\frac{e^{(\lg(a))^2}}{e^{\frac{\lg(|K(G)|)}{k}}} < 1/4$. Hence $\ln(4) < \frac{\lg(|K(G)|)}{k} - (\lg(a))^2$. Hence $k < \frac{\lg|K(G)|}{\ln(4)+(\lg(a))^2}$. □

Lemma 2.2. *Suppose G is a finite group and H is the hidden subgroup. Then we can retrieve $core_G(H)$ after $m = 2l\lg(|\ G\ |)$ steps with probability $1 - e^{-\frac{lg(|G|)}{4l}{(l-1)^2}}$*

Proof. The proof is the same as the proof of Theorem 5 in (**?**) with $k = 2l\lg(|\ G\ |)$ and $\lambda = (l-1)\lg(|\ G\ |)$. Following the proof we conclude that the probability of obtaining $core_G(H)$ is $1 - e^{-\frac{lg(|G|)}{4l}{(l-1)^2}}$. □

Theorem 2.3. *Suppose G is a finite group and $a = [G : K(G)]$. If we repeat Quantum Fourier Sampling $m = 2l\lg(|\ G\ |)$ times where $l = (8\lceil\frac{\ln(4)+\lg^2(a)}{\lg(|K(G)|)}\rceil + 8)$ for all subgroups of G containing $K(G)$ we can retrieve H in the "almost abelian" algorithm with probability greater than $1/2$.*

Proof. We first note that

$$\frac{4l}{(l-1)^2} = \frac{32\lceil\frac{\ln(4)+\lg^2(a)}{\lg(|K(G)|)}\rceil + 32}{(8\lceil\frac{\ln(4)+\lg^2(a)}{\lg(|K(G)|)}\rceil + 7)^2} < \frac{32\lceil\frac{\ln(4)+\lg^2(a)}{\lg(|K(G)|)}\rceil + 32}{49(\lceil\frac{\ln(4)+\lg^2(a)}{\lg(|K(G)|)}\rceil + 1)^2}$$

$$< \frac{32}{49(\lceil\frac{\ln(4)+\lg^2(a)}{\lg(|K(G)|)}\rceil)} < \frac{32}{49}\frac{\lg\mid K(G)\mid}{\ln(4)+(\lg(a))^2}.$$

If the algorithm is run for m steps for all subgroups of G containing $K(G)$ then the probability of retrieving H^G for each of these subgroups will be $1 - e^{-\frac{lg(|G|)}{4l}{(l-1)^2}}$ which, by the above computation, is bigger than $1 - e^{-\frac{lg(|G|)}{l'}}$ where $l' = \frac{32}{49}\frac{\lg|K(G)|}{\ln(4)+(\lg(a))^2}$. Since the number

of subgroups of a group of order a cannot exceed $2^{\lg^2(a)}$, by Lemma 4.1 it is clear that we can retrieve H at the end of the "almost abelian" algorithm with probability bigger than $1/2$. □

2.2 An Almost Abelian Group of Order $3 \cdot 2^n$

We now analyze the quantum algorithm for finding the hidden subgroups of the almost abelian group $G = \mathbb{Z}_3 \rtimes \mathbb{Z}_m$ where $m = 2^n$. These groups are mentioned as examples of almost abelian groups in (11). For each non-trivial subgroup, we calculate the probabilities that the algorithm yields any particular subgroup after i steps. These probabilities are given in Appendix A.

The subgroups of the group G are as follows. We denote by Z_0 the unique normal subgroup of the sylow 2-subgroups of index 2. We denote by T the sylow 3-subgroup of G, by SY_i where $i = 1, 2, 3$ the three sylow 2-subgroups. Apart from these the subgroups of TZ_0 and Z_0 are also subgroups of G. If $N(H)$ denote the normalizer of a subgroup H of G we have that $\bigcap_H N(H) = Z_0$.

G has m linear characters and $m/2$ non-linear characters of degree 2 induced from the characters of TZ_0 where T is the sylow 3-subgroup of G. In this section we explicitly calculate, given any hidden subgroup, the probabilities of getting the subgroup after i steps as the intersection of the possible kernels of the irreducible representations measured corresponding to all the subgroups of G containing Z_0.

Theorem 2.4. *Let $G = \mathbb{Z}_3 \rtimes \mathbb{Z}_m$ be an almost abelian group. Let H be a non-trivial subgroup of G. Run the almost abelian algorithm i times. Then the probability of the process yielding any particular subgroup of G is given by the Tables in Appendix A ($A - i$ where $i = 1, \ldots 15$).*

Proof. 1) When $H = SY_1$ and $\overline{G} = TZ_0$. The probability of getting an irreducible representation ρ is given by $\frac{d_\rho}{|\overline{G}|} \sum_{h \in H \bigcap \overline{G}} \chi_\rho(h)$. Hence the probability is equal to $\frac{1}{3m/2}.m/2 = 1/3$ when Z_0 is in the kernel of χ_ρ otherwise the probability is equal to

0. The possible kernels are TZ_0 and Z_0. So after the first iteration the probabilities of getting kernels such that $\mid ker(\chi_\rho) \mid = 3^a 2^N$ are

$$p(a,N) = \begin{cases} 1/3 & N = n-1, a = 1 \\ 2/3 & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

After i iterations the probabilities are given by

$$p(a,N) = \begin{cases} (1/3)^i & N = n-1, a = 1 \\ 1-(1/3)^i & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

When $\overline{G} = Z_0$. The probability of getting a non-trivial irreducible representation is 0. The trivial representation is measured with probability 1. The only possible kernel is Z_0. After i iterations the probability of getting Z_0 is 1.

When $\overline{G} = SY_1$. The probability of getting any non-trivial irreducible representation is 0. The probability of measuring the trivial representation is 1. The possible kernel is SY_1. After i iterations the probability of getting SY_1 is 1.

When $\overline{G} = SY_2$. The probability of measuring an irreducible representation ρ is given by 1/2. So after i steps the probabilities of getting the intersection of the kernels to be of order 2^N are given by

$$p(N) = \begin{cases} (1/2)^i & N = n \\ 1-(1/2)^i & N = n-1 \\ 0 & otherwise \end{cases}$$

When $\overline{G} = SY_3$. The probabilities that we get are the same as above.

When $\overline{G} = G$. If χ_ρ is linear then $\frac{d_\rho}{|G|}\sum_{h\in H}\chi_\rho(h) = 1/3$ if $\chi_\rho = 1_G$ and 0 otherwise. Suppose χ_ρ is non-linear. Then $\chi_\rho = \lambda^G$ where $\lambda \in Irr(TZ_0)$. Now

$$\frac{d_\rho}{|\ G\ |}\sum_{h\in H}\chi_\rho(h) = 2\frac{|\ H\ |}{|\ G\ |}((\chi_\rho)_H, 1_H) = 2/3((\chi_\rho)_H, 1_H) = 2/3((\lambda^G)_H, 1_H)$$

$$= 2/3((\lambda_{H\bigcap TZ_0})^H, 1_H) = 2/3(\lambda_{H\bigcap TZ_0}, 1_{Z_0})$$

$$= 2/3(\lambda_{Z_0}, 1_{Z_0}) = 0$$

if $\lambda_{Z_0} \neq 1_{Z_0}$ and 2/3 if $\lambda_{Z_0} = 1_{Z_0}$. The possible kernels are G and Z_0.

After the first iteration the probabilities of getting $|\ ker(\chi_\rho)\ | = 3^a 2^N$ re given by

$$p(a, N) = \begin{cases} (1/3) & N = n, a = 1 \\ (2/3) & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

After i iterations the probabilities will be

$$p(a, N) = \begin{cases} (1/3)^i & N = n, a = 1 \\ 1-(1/3)^i & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

$H = TZ_0$.

1) When $\overline{G} = Z_0$. Then the probability of measuring the trivial representation is 1. The possible kernel is Z_0. The probability that the intersection of the kernels will be Z_0 after i iterations is 1.

2) When $\overline{G} = TZ_0$. The probability of measuring the trivial representation is 1. The only possible kernel is TZ_0. The probability that after i iterations the intersection of the kernels is TZ_0 is 1.

3) When $\overline{G} = SY_1$. The probability of measuring a non-trivial representation ρ is given by

$$\frac{1}{\mid SY_1 \mid} \sum_{h \in Z_0} \chi_\rho(h).$$

So the probability is $1/2$ if $Z_0 \in ker(\chi_\rho)$ and 0 otherwise. So the possible kernels are Z_0 and SY_1. So after the first iteration the probabilities that the $\mid ker(\chi_\rho) \mid = 2^N$ are

$$p(a, N) = \begin{cases} (1/2) & N = n \\ (1/2) & N = n-1 \\ 0 & otherwise \end{cases}$$

After i iterations the probabilities are

$$p(a, N) = \begin{cases} (1/2)^i & N = n \\ (1/2)^i(2^i - 1) & N = n-1 \\ 0 & otherwise \end{cases}$$

4) When $\overline{G} = G$. Then the probability of measuring an irreducible representation ρ is 1/2. Hence if the kernels are given by $\mid ker(\chi_\rho) \mid = 3.2^N$ then the probabilities of getting the intersection to be one of them after i iterations are

$$p(a, N) = \begin{cases} (1/2)^i & N = n \\ (1/2)^i(2^i - 1) & N = n-1 \\ 0 & otherwise \end{cases}$$

When $H = Z_0$.

1) $\overline{G} = TZ_0$. Then the probability of measuring an irreducible representation ρ of TZ_0 is 1/3 when $Z_0 \in ker(\chi_\rho)$ and 0 otherwise. The possible kernels are TZ_0 and Z_0.

After i iterations the probabilities of getting $\mid ker(\chi_\rho) \mid = 3^a 2^N$ are

$$p(a,N) = \begin{cases} (1/3)^i & N = n-1, a = 1 \\ 1-(1/3)^i & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

2) $\overline{G} = Z_0$. The probability of measuring the trivial representation is 1 and 0 otherwise. So after i iterations the probabilities that $\mid ker(\chi_\rho) \mid = 2^N$ are

$$p(a,N) = \begin{cases} 1 & N = n-1 \\ 0 & otherwise \end{cases}$$

3) $\overline{G} = SY_1$. The probability of measuring an irreducible representation ρ of SY_1 is 1/2 if Z_0 is in kernel of χ_ρ and 0 otherwise. The possible kernels of χ_ρ are SY_1 and Z_0. the probabilities after i iterations of getting $\mid ker(\chi_\rho) \mid = 2^N$ are

$$p(a,N) = \begin{cases} (1/2)^i & N = n \\ (1/2)^i(2^i-1) & N = n-1 \\ 0 & otherwise \end{cases}$$

If $\overline{G} = g_1 SY_1 (g_1)^{-1}$ the probabilities are going to be the same.

4) $\overline{G} = G$. The probability of measuring an irreducible representation ρ is 1/6 if χ_ρ is linear and contains Z_0 in its kernel and 2/3 if it is non-linear and contains Z_0 in its kernel and 0 otherwise. The possible kernels are Z_0, TZ_0 and G. So the probabilities that $\mid ker(\chi_\rho) \mid = 3^a 2^N$ are

$$p(a,N) = \begin{cases} (1/6) & N = n, a = 1 \\ (1/6) & N = n-1, a = 1 \\ 2/3 & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

So after i iterations the probabilities are

$$p(a,N) = \begin{cases} (1/6)^i & N = n, a = 1 \\ (1/6)^i(2^i - 1) & N = n-1, a = 1 \\ (1 - \frac{1}{3^i}) & N = n-1, a = 0 \\ 0 & otherwise \end{cases}$$

When $H < TZ_0$ and $\mid H \mid = 3.2^N$.

1) When $\overline{G} = TZ_0$. The probability of measuring an irreducible representation ρ is

$$\frac{1}{\mid TZ_0 \mid} \sum_{h \in H} \chi_\rho(h) = 2^{k+1}/2^n = 2^{k+1-n}$$

if $H \in ker(\chi_\rho)$ and equal to 0 otherwise. So the probabilities that $\mid ker(\chi_\rho) \mid = 3.2^N$ are

$$p(N) = \begin{cases} 0 & N < k \\ 2^{k+1-n} & N = n-1 \\ \frac{1}{2^{N-k+1}} & k \leq N < n-1 \end{cases}$$

After i iterations the probability that the intersection of the kernels is H is given by

$$1 - [p(N \neq k)]^i = 1 - (1/2)^i.$$

The probability that the intersection is TZ_0 is given by $[p(N = n-1)]^i$. The probability that the intersection is a subgroup of TZ_0 of order 3.2^m where $k < m < n-1$ is given by

$$p(N \geq m) - p(N > m) = [\frac{2}{2^{m-k+1}}]^i - [\frac{1}{2^{m-k+1}}]^i = [\frac{1}{2^{m-k+1}}]^i (2^i - 1)$$

Hence we have after i iterations

$$p(N) = \begin{cases} 0 & N < k \\ (2^{k+1-n})^i & N = n-1 \\ (\frac{1}{2^{m-k+1}})^i (2^i - 1) & k < m < n-1 \\ (1 - [1/2]^i) & N = k \end{cases}$$

2) When $\overline{G} = Z_0$. The probability of measuring an irreducible representation ρ is

$$\frac{1}{\mid Z_0 \mid} \sum_{h \in H \bigcap Z_0} \chi_\rho(h) = 2^{k+1}/2^n = 1/2^{n-k-1}$$

if $H \bigcap Z_0 \in ker(\chi_\rho)$ and 0 otherwise. So the probabilities that $\mid ker(\chi_\rho) \mid = 2^N$ are

$$p(N) = \begin{cases} 0 & N < k \\ 2^{k+1-n} & N = n-1 \\ \frac{1}{2^{N-k+1}} & k \leq N < n-1 \end{cases}$$

After i iterations the probability that the intersection of the kernels is Z_0 is $[1/2^{n-k-1}]^i$. The probability that the intersection is a subgroup of Z_0 of order 2^m where $k < m < n-1$ is $[1/2^{m-k+1}]^i(2^i - 1)$. Hence after i iterations we have

$$p(N) = \begin{cases} 0 & N < k \\ (2^{k+1-n})^i & N = n-1 \\ (\frac{1}{2^{m-k+1}})^i(2^i - 1) & k < m < n-1 \\ (1 - [1/2]^i) & N = k \end{cases}$$

3) When $\overline{G} = SY_1$. The probability of measuring an irreducible representation ρ is given by

$$\frac{1}{\mid SY_1 \mid} \sum_{h \in H \bigcap SY_1} \chi_\rho(h) = 2^k/2^n = 1/2^{n-k}$$

if $H \bigcap SY_1 \in ker(\chi_\rho)$ and 0 otherwise. So the probabilities that $\mid ker(\chi_\rho) \mid = 2^N$ are

$$p(N) = \begin{cases} 0 & N < k \\ 1/2^{n-k} & N = n \\ \frac{1}{2^{N-k+1}} & k \leq N < n \end{cases}$$

The probabilities after i iterations are

$$p(N) = \begin{cases} 0 & N < k \\ (1/2^{n-k})^i & N = n \\ (\frac{1}{2^{m-k+1}})^i(2^i - 1) & k < m < n \\ (1 - [1/2]^i) & N = k \end{cases}$$

4) When $\overline{G} = G$. Then the probability of measuring an irreducible representation ρ of G is $2^k/2^n = 1/2^{n-k}$ if $H \in ker(\chi_\rho)$ and 0 otherwise. The probabilities that $\mid ker(\chi_\rho) \mid = 3.2^N$ are given by

$$p(N) = \begin{cases} 0 & N < k \\ 1/2^{n-k} & N = n \\ \frac{1}{2^{N-k+1}} & k \leq N < n \end{cases}$$

After i steps the probabilities are

$$p(N) = \begin{cases} 0 & N < k \\ (1/2^{n-k})^i & N = n \\ (\frac{1}{2^{m-k+1}})^i(2^i - 1) & k < m < n \\ (1 - [1/2]^i) & N = k \end{cases}$$

When $H < Z_0$ and $\mid H \mid = 2^k$

1) When $\overline{G} = TZ_0$. The probability of measuring an irreducible representation ρ is given by

$$\frac{d_\rho}{\mid TZ_0 \mid} \sum_{h \in H} \chi_\rho(h) = \frac{1}{3} 2^{k-n+1}$$

if $H \in ker(\chi_\rho)$ and 0 otherwise. The probabilities that $\mid ker(\chi_\rho) \mid = 3^a 2^N$ are given by

$$p(a,N) = \begin{cases} 0 & N < k \\ \frac{1}{3.2^{n-k-1}} & N = n-1, a = 1 \\ \frac{2^{k-N-1}}{3} & k \leq N < n-1, a = 1 \\ \frac{2^{k-N}}{3} & k \leq N < n-1, a = 0 \\ \frac{1}{3.2^{n-k-2}} & N = n-1, a = 0 \end{cases}$$

This probability distribution is a product of two independent probability distributions $p_{0,3}(i)$ and $p_{0,2}(i)$ where

$$p_{0,3}(i) = \begin{cases} 2/3 & i = 0 \\ 1/3 & i = 1 \end{cases}$$

and

$$p_{0,2}(i) = \begin{cases} 0 & i < k \\ 1/2^{n-k-1} & i = n-1 \\ 2^{k-i-1} & i < n-1 \end{cases}$$

After i iterations the probability that the intersection of the kernels is TZ_0 is $\frac{1}{3^i}\frac{1}{(2^{n-k-1})^i}$. The probability that the intersection is Z_0 is $(1-\frac{1}{3^i})(\frac{1}{(2^{n-k-1})^i}$. The probability that the intersection is H is $(1-\frac{1}{3^i})(1-\frac{1}{2^i})$. The probability that the intersection is a subgroup of TZ_0 of order 3.2^m is given by $\frac{1}{3^i}(2^i-1)\frac{1}{(2^{m-k+1})^i}$ and the probability that the intersection of kernels is a subgroup of Z_0 of order 2^m is given by $(1-\frac{1}{3^i})(2^i-1)\frac{1}{(2^{m-k+1})^i}$. Hence we have

$$p(a,N) = \begin{cases} 0 & N < k \\ \frac{1}{3^i}\frac{1}{(2^{n-k-1})^i} & N = n-1, a = 1 \\ (1-\frac{1}{3^i})\frac{1}{(2^{n-k-1})^i} & N = n-1, a = 0 \\ (1-\frac{1}{3^i})(1-\frac{1}{2^i}) & N = k, a = 0 \\ \frac{1}{3^i}(1-\frac{1}{2^i}) & N = k, a = 1 \\ \frac{1}{3^i}(2^i-1)(\frac{1}{2^{m-k+1}})^i & N = m, a = 1, k < m < n-1 \\ (1-\frac{1}{3^i})(2^i-1)(\frac{1}{2^{m-k+1}})^i & N = m, a = 0 \end{cases}$$

2) When $\overline{G} = SY_1$. The probability of measuring any irreducible representation ρ is $1/2^{n-k}$ if H is in the kernel of χ_ρ and 0 otherwise. So the probabilities that $\mid ker(\chi_\rho) \mid = 2^N$ are given by

$$p(N) = \begin{cases} 0 & N < k \\ (1/2^{n-k}) & N = n \\ (\frac{1}{2^{N-k+1}}) & k \leq N < n \end{cases}$$

After i iterations the probabilities that the intersection of the kernels have order 2^N are given by

$$p(N) = \begin{cases} 0 & N < k \\ (1/2^{n-k})^i & N = n \\ (1 - \frac{1}{2^i}) & N = k \\ \frac{1}{(2^{m-k+1})^i}(2^i - 1) & k < m < n \end{cases}$$

3) When $\overline{G} = Z_0$. The probability of measuring any irreducible representation ρ of Z_0 is given by $1/2n - k - 1$ if H is contained in the kernel of χ_ρ and 0 otherwise. The probabilities that $\mid ker(\chi_\rho) \mid = 2^N$ are given by

$$p(N) = \begin{cases} 0 & N < k \\ (1/2^{n-k-1}) & N = n-1 \\ \frac{1}{2^{N-k+1}} & k \leq N < n-1 \end{cases}$$

After i steps the probabilities of the intersection of the kernels are

$$p(N) = \begin{cases} 0 & N < k \\ (1/2^{n-k-1})^i & N = n-1 \\ (1 - \frac{1}{2^i}) & N = k \\ \frac{1}{(2^{m-k})^i}(1 - \frac{1}{2^i}) k < m < n-1 \end{cases}$$

4) When $\overline{G} = G$. The probability of measuring an irreducible representation ρ is given by

$$\frac{d_\rho}{\mid G \mid} \sum_{h \in H} \chi_\rho(h).$$

When ρ is linear then the probability is $2^k/3.2^n = \frac{1}{3}2^{k-n}$ if $ker(\chi_\rho)$ contains H and it is $\frac{1}{32^{n-k-2}}$ if ρ is nonlinear and its kernel contains H. So we have the following for the probabilities of getting $|\ \ker(\chi_\rho)\ | = 3^a 2^N$

$$p(a,N) = \begin{cases} 0 & N < k \\ \frac{1}{3}2^{k-N-1} & k \leq N \leq n-1, a = 1 \\ \frac{1}{3}2^{k-n} & N = n, a = 1 \\ 0 & N = n, a = 0 \\ \frac{1}{3}2^{k-n+2} & N = n-1, a = 0 \\ \frac{1}{3}2^{k-N} & k \leq N < n-1, a = 0 \end{cases}$$

After i iterations the probability that intersection of kernels have order $3^a 2^N$ is $(p(a,N))^i - (p(a+1,N))^i - (p(a,N+1))^i + (p(a+1,N+1))^i$. Hence we have

$$p(a,N) = \begin{cases} 0 & N < k \\ (\frac{2^{k-n+1}}{3})^i - (\frac{2^{k-n}}{3})^i & N = n-1, a = 1 \\ (2^{k-m})^i - (\frac{2^{k-m}}{3})^i - (2^{k-m-1})^i + (\frac{2^{k-m-1}}{3})^i & k \leq m < n-1, a = 0 \\ (\frac{2^{k-m}}{3})^i - (\frac{2^{k-m-1}}{3})^i & k \leq m < n-1, a = 1 \\ (2^{k-n+1})^i - (\frac{2^{k-n+1}}{3})^i & N = n-1, a = 0 \\ 0 & N = n, a = 0 \\ \frac{1}{3^i}(\frac{1}{2^{n-k}})^i & N = n, a = 1 \end{cases}$$

□

CHAPTER 3
KEMPE-SHALEV DISTINGUISHABLITY

For the remainder of this work, we consider the decision version of the Hidden Subgroup problem. As we saw, it is stated as follows.

Decision Version of the Hidden Subgroup Problem : Let G be a finite group and H a subgroup. Given a black-box function $f : G \to S$ which is constant on (left)-cosets gH of H and takes different values for different cosets, determine whether $H = \{e\}$ or not.

There are two ways to formalize the existence of solutions to this problem. In this chapter, we discuss the definition given by Kempe and Shalev (18). A different way to define this will be discussed in the next chapter. Kempe and Shalev propose that if the subgroup H of G produces probabilities of representations under Quantum Fourier Sampling that are very close to those that arise from the trivial subgroup, then the subgroup should be called indistinguishable from the trivial subgroup. More precisely, the definition proposed by Kempe and Shalev (18) in 2005 is as follows.

Definition 4. Let G be a finite group. Let $\mathrm{Irr}(G)$ be the set of irreducible (complex) representations of G. We denote by χ_ρ the character associated to a $\rho \in \mathrm{Irr}(G)$ and let d_ρ be it's degree. For $H < G$ we define

$$\mathbf{D}_H = \frac{1}{\mid G \mid} \sum_{\rho \in \mathrm{Irr}(G)} d_\rho \mid \sum_{h \neq e, h \in H} \chi_\rho(h) \mid .$$

We say that a subgroup H is distinguishable if $\mathbf{D}_H \geq log(\mid G \mid)^{-c}$ for some $c > 0$, c being independent of G.

We begin this section by proving that all subgroups of an abelian group are Kempe-Shalev distinguishable.

Theorem 3.1. *Subgroups of an abelian group G are Kempe-Shalev distinguishable.*

Proof. Let H be a hidden subgroup of the abelian group G. Then

$$D_H = \frac{1}{|G|}\sum_{\rho} d_\rho |\sum_{h\neq e}\chi_\rho(h)|$$

$$= \frac{1}{|G|}\sum_{\rho}|\sum_{h\neq e}\chi_\rho(h)| = \frac{1}{|G|}[\sum_{\rho,ker(\rho)\supseteq H}|\sum_{h\neq e}\chi_\rho(h)| + \sum_{\rho,ker(\rho)\not\supseteq H}|\sum_{h\neq e}\chi_\rho(h)|]$$

$$= \frac{1}{|G|}[\sum_{\rho,ker(\rho)\supseteq H}||H| < (\chi_\rho)_H, 1_H > -\chi_\rho(1)| + \sum_{\rho,ker(\rho)\not\supseteq H}||H| < (\chi_\rho)_H, 1_H > -\chi_\rho(1)|]$$

$$= \frac{1}{|G|}[\sum_{\rho,ker(\rho)\supseteq H}||H|\chi_\rho(1) - \chi_\rho(1)| + \sum_{\rho,ker(\rho)\not\supseteq H}|\chi_\rho(1)|]$$

$$= \frac{1}{|G|}[\sum_{\rho,ker(\rho)\supseteq H}\chi_\rho(1)[|H|-1] + \sum_{\rho,ker(\rho)\not\supseteq H}\chi_\rho(1)]$$

$$= \frac{1}{|G|}[\sum_{\rho,ker(\rho)\supseteq H}[|H|-1] + \sum_{\rho,ker(\rho)\not\supseteq H}1]$$

$$= \frac{1}{|G|}[|G|/|H|[|H|-1]+(|G|-|G|/|H|)] = 2\frac{1}{|G|}(|G|-|G|/|H|) = 2(1-\frac{1}{|H|}) > 1 > (\log(|G|)^{-c}$$

for each $c > 0$ as $|G| \to \infty$.

□

In this chapter we study the distinguishability of subgroups of Frobenius groups using the old definition of distinguishability. Here we consider Frobenius groups with abelian kernel. We give necessary and sufficient conditions for the distinguishability of the subgroups of the Frobenius groups under certain conditions.

Definition 5. Let G be a finite group. Let $H \subseteq G$ and H is a nontrivial proper subgroup of G. Assume that $H \cap H^g = 1$ whenever $g \in G - H$. Then H is a Frobenius complement in G. A group which contains a Frobenius complement is called a Frobenius group.

Theorem 3.2 (Frobenius)**.** *Let G be a Frobenius group with complement H. Then there exists $K \lhd G$ with $HK = G$ and $H \cap K = 1$.*

Proof. See (16). □

This subgroup K is called the Frobenius kernel of G. It is clear that a Frobenius group with kernel K and complement H can be written as $K \rtimes H$. It also follows that any non-trivial element of H fixes no element of K i.e H acts semiregularly on K.

Theorem 3.3. *Let $G = {\mathbb{Z}_{\alpha(\beta)}}^{g(\beta)} \rtimes \mathbb{Z}_\beta$ be a Frobenius group where $g(\beta)$ is a function of β and $\alpha(\beta)$ is coprime to β, and for some $c > 0$ and for all sufficiently large β, $g(\beta) > \beta^{\frac{1}{c}}$. Let H be a subgroup of order $\alpha(\beta)^{f(\beta)}$ or $\beta.\alpha(\beta)^{f(\beta)}$ where $f(\beta)$ is a function of β such that $0 \leq f(\beta) \leq g(\beta)$ then H is Kempe-Shalev distinguishable if and only if $f(\beta) > 0$ for all $\beta >> 0$.*

Proof. Suppose $f(\beta) > 0$ for $\beta >> 0$, and take β sufficiently large. Then $f(\beta) > 0$ and H has order divisible by α which is coprime to β. Furthermore for each $\rho \in Irr(G)$

$$| \sum_{h \neq e, h \in H} \chi_\rho(h) | = | H | [(\chi_\rho)_H, 1_H] - \chi_\rho(1) | \geq 1,$$

since *alpha* divides $| H |$ and is coprime to $\chi_\rho(1)$. Hence

$$\sum_{\rho = \text{non-linear}} | \sum_{h \neq e, h \in H} \chi_\rho(h) | \geq \frac{\alpha(\beta)^{g(\beta)} - 1}{\beta}.$$

Hence

$$\mathbf{D}_H \geq \frac{\beta(| H | -1) + \beta(\frac{\alpha^{g(\beta)}-1}{\beta})}{\beta.\alpha(\beta)^{g(\beta)}} > \frac{(\alpha(\beta)^{g(\beta)} - 1) + 1}{\beta.\alpha(\beta)^{g(\beta)}} = \frac{1}{\beta} > \frac{1}{(log \mid G \mid)^c}$$

for some $c > 0$. Hence H is distinguishable. If $f(\beta)$=0 then H has order either $\alpha^{f(\beta)} = 1$ or $\beta.\alpha(\beta)^{f(\beta)} = \beta$.In this case

$$\mathbf{D}_H \leq \frac{2(\beta - 1)}{\alpha(\beta)^{g(\beta)}.\beta},$$

and for each $c > 0$ and sufficiently large β, we have

$$\frac{2(\beta-1)}{\alpha(\beta)^{g(\beta)}.\beta} < (log(\mid G \mid))^{-c}.$$

Therefore,if $f(\beta) = 0$ infinitely often, H is indistinguishable. Hence the proof. □

Corollary 3.4. *The Frobenius complement of G is indistinguishable.*

Proof. The Frobenius complement of G has order β. Hence $f(\beta) = 0$. From the previous theorem the complement is indistinguishable. □

Corollary 3.5. *The Frobenius kernel of G is Kempe-Shalev distinguishable.*

Proof. The order of the Frobenius kernel is $\alpha(\beta)^{g(p)}$. Hence the corollary follows from the previous theorem. □

Proposition 3.6. *For the frobenius group ${\mathbb{Z}_2}^{p-1} \rtimes \mathbb{Z}_p$ the smallest $\mathbf{D}_S$ for S a non-trivial subgroup is obtained when the subgroup S is the Sylow p– subgroup of the group.*

Proof. From the character table it is evident that when S is the Sylow p–subgroup then $\sum_\rho d_\rho \mid \sum_{h\neq e, h\in S} \chi(\rho) \mid$ =2$(p-1)$ the contribution from non-linear characters being zero. So $\mathbf{D}_S$ = $\frac{2(p-1)}{2^{p-1}.p}$. Now if H is a subgroup with $\mid H \mid = 2^k$ then $\mathbf{D}_H$= $\frac{p(2^k-1)+....}{2^{p-1}.p}$ where $p(2^k-1)$ is the contribution from linear characters. This $\mathbf{D}_H$ is obviously bigger than $\mathbf{D}_S$ when k>1. If k=1 then $\mid H \mid$=2 and $\mathbf{D}_H$ = $\frac{(p-1)+p.x}{2^{p-1}.p}$ where $x = \sum_{\rho=\text{non-linear}} \mid \sum_{h\neq e, h\in H} \chi(\rho) \mid$>0. This sum is equal to $\sum_{\rho=\text{non-linear}} \mid\mid H \mid [(\chi_\rho)_H, 1_H] - \chi_\rho(1) \mid$ which is bigger than 1 because $\mid H \mid [(\chi_\rho)_H, 1_H] - \chi_\rho(1)$ is never equal to zero and bigger than 1. Hence this is also bigger than $\mathbf{D}_S$. Any other subgroup of G will be of the form $H \backsimeq {\mathbb{Z}_2}^k \rtimes \mathbb{Z}_p$. This subgroup H has $2^k - 1$ elements of order 2 and so $\mathbf{D}_H$= $\frac{p(2^k-1)+....}{2^{p-1}.p}$. Since $k > 1$ this is greater than $\mathbf{D}_S$. □

Lemma 3.7. *Let $\alpha > 1$ be a constant,and let m, n, g be non-negative real valued functions of* **N***. Assume that $m(i), n(i) \to \infty$ as $i \to \infty$. Also assume that there exists*

some $c_0 > 0$ *such that* $g(i)^{c_0} > m(i)n(i)$ *for all sufficiently large* i*. Then for each* $c > 0$ $\frac{\alpha^{g(i)}}{m(i)n(i)} > g(i)^c$ *for all sufficiently large* i*.*

Proof. Let $c > 0$. For all sufficiently large i,we have $\alpha^{g(i)} > g(i)^{c+c_0}$. Hence for all sufficiently large i we have

$$\alpha^{g(i)} > g(i)^{c+c_0} = g(i)^c g(i)^{c_0} > g(i)^c m(i)n(i)$$

Hence $\frac{\alpha^{g(i)}}{m(i)n(i)} > g(i)^c$. □

Theorem 3.8. *Let* $G = \mathbb{Z}_\alpha{}^{g(i)} \rtimes \mathbb{Z}_{m(i)} \rtimes \mathbb{Z}_{n(i)}$ *be a Frobenius group where* $(m(i), n(i)) = 1$ *and* α *is coprime to* $m(i)$ *and* $n(i)$*.Assume that* $m(i), n(i) \to \infty$ *as* $i \to \infty$*. Also assume that for some* $c > 0$ $g(i)^c \geq m(i)n(i)$ *and for sufficiently large* i*. Let* H *be a subgroup of order* $\alpha^{f(i)}$ *or* $\alpha^{f(i)}.m(i)$ *or* $\alpha^{f(i)}.n(i)$ *or* $\alpha^{f(i)}.m(i)n(i)$*. Then* H *is distinguishable iff* $f(i) > 0$ *for all sufficiently large* $i > 0$*.*

Proof. Let $f(i) > 0$ and take i sufficiently large. Then H has order divisible by α which is coprime to $m(i)$ and $n(i)$. Therefore for each $\rho \in Irr(G)$

$$| \sum_{h \neq e, h \in H} \chi_\rho(h) | = | H | [(\chi_\rho)_H, 1_H] - \chi_\rho(1) | \geq 1.$$

Hence

$$\sum_{\rho=\text{non-linear of degree m(i)n(i)}} | \sum_{h \neq e, h \in H} \chi_\rho(h) | \geq \frac{\alpha^{g(n)} - 1}{mn}.$$

Hence

$$\mathbf{D}_H = \frac{\sum_{\rho=\text{linear}} | \sum_{h \neq e, h \in H} \chi_\rho(h) | + \sum_{\rho=\text{non-linear}} d_\rho | \sum_{h \neq e, h \in H} \chi_\rho(h) |}{\alpha^{g(i)}.m(i)n(i)}.$$

Hence

$$\begin{aligned} \mathbf{D}_H &\geq \frac{1 + \sum_{\rho=\text{non-linear}} d_\rho | \sum_{h \neq e, h \in H} \chi_\rho(h) |}{\alpha^{g(i)}.m(i)n(i)} \\ &\geq \frac{1 + m(i)n(i) \sum_{\rho=\text{non-linear of degree m(i)n(i)}} 1}{\alpha^{g(i)}.m(i)n(i)} \end{aligned}$$

$$\geq \frac{1 + m(i)n(i).\frac{\alpha^{g(i)}-1}{m(i)n(i)}}{\alpha^{g(i)}.m(i)n(i)} = \frac{1}{m(i)n(i)}$$

which is evidently bigger than $log(\mid G \mid)^{-c}$ from hypotheses. If $f(i) = 0$ then $\mid H \mid = m(i)$ or $n(i)$ or $m(i)n(i)$. If $\mid H \mid = m(i)$ then

$$\mathbf{D}_H \leq \frac{n(i)(m(i)-1) + n(i)(m(i)-1)n(i)(m(i)-1)}{\alpha^{g(i)}m(i)n(i)}$$

$$= \frac{n(i)(m(i)-1)}{\alpha^{g(i)}m(i)n(i)} + \frac{n(i)^2(m(i)-1)^2}{\alpha^{g(i)}m(i)n(i)}$$

$$\leq \frac{1}{\alpha^{g(i)}} + \frac{m(i)n(i)}{\alpha^{g(i)}}$$

$$\leq (log \mid G \mid)^{-c}$$

for each $c > 0$ and sufficiently large i from Lemma 3.7. If $\mid H \mid = n(i)$ then

$$\mathbf{D}_H \leq \frac{2(n(i)-1) + n(i)(m(i)-1)n(i)(n(i)-1)}{\alpha^{g(i)}m(i)n(i)} = \frac{2}{\alpha^{g(i)}m(i)} - \frac{2}{\alpha^{g(i)}m(i)n(i)} + \frac{n(i)^2}{\alpha^{g(i)}} \leq (log \mid G \mid)^{-c}$$

for each $c > 0$ and sufficiently large $n(i)$. If $\mid H \mid = m(i)n(i)$ then

$$\mathbf{D}_H \leq \frac{(m(i)n(i)-1) + (n(i)-1)m(i)n(i) + n(i)\frac{m(i)-1}{n(i)}n(i)}{\alpha^{g(i)}m(i)n(i)}$$

$$\leq \frac{n(i)}{\alpha^{g(i)}} + \frac{1}{\alpha^{g(i)}} - \frac{1}{\alpha^{g(i)}m(i)}$$

$$\leq (log \mid G \mid)^{-c}$$

for each $c > 0$ and sufficiently large i from Lemma 3.7. Hence the proof. □

Theorem 3.9. *Let* $G = \mathbb{Z}_\alpha{}^{g(i)} \rtimes (SL(2,5) \times (\mathbb{Z}_{m(i)} \rtimes \mathbb{Z}_{n(i)}))$ *be a Frobenius group where* $i \in \mathbb{N}, (m(i), n(i)) = 1$ *and* $\alpha > 1$ *is a constant and coprime to* $m(i)$ *and* $n(i)$*.Assume that* $m(i), n(i) \to \infty$ *as* $i \to \infty$*. Also assume that for some* $c > 0$ $g(i)^c \geq m(i)n(i)$ *for all sufficiently large* i*. Let* H *be a subgroup of order* $\alpha^{f(i)}$ *or* $\alpha^{f(i)}.m(i)$ *or* $\alpha^{f(i)}.n(i)$ *or* $\alpha^{f(i)}.m(i)n(i)$ *or* $\alpha^{f(i)}120m(i)$ *or* $\alpha^{f(i)}120n(i)$*. Then* H *is Kempe-Shalev distinguishable iff* $f(i) > 0$ *for all sufficiently large* i*.*

Proof. Let $f(i) > 0$ and take i sufficiently large. Then H has order divisible by α which is coprime to $m(i)$ and $n(i)$. Therefore for each $\rho \in Irr(G)$

$$| \sum_{h \neq e, h \in H} \chi_\rho(h) | = || H | [(\chi_\rho)_H, 1_H] - \chi_\rho(1) | \geq 1.$$

Hence

$$\sum_{\rho=\text{non-linear of degree 120m(i)n(i)}} | \sum_{h \neq e, h \in H} \chi_\rho(h) | \geq \frac{\alpha^{g(i)} - 1}{120m(i)n(i)}.$$

Hence

$$\mathbf{D}_H = \frac{\sum_{\rho=\text{linear}} | \sum_{h \neq e, h \in H} \chi_\rho(h) | + \sum_{\rho=\text{non-linear}} d_\rho | \sum_{h \neq e, h \in H} \chi_\rho(h) |}{\alpha^{g(i)}.120m(i)n(i)}.$$

Hence

$$\begin{aligned} \mathbf{D}_H &\geq \frac{1 + \sum_{\rho=\text{non-linear}} d_\rho | \sum_{h \neq e, h \in H} \chi_\rho(h) |}{\alpha^{g(i)}.120m(i)n(i)} \\ &\geq \frac{1 + m(i)n(i) \sum_{\rho=\text{non-linear of degree 120m(i)n(i)}} 1}{\alpha^{g(i)}.120m(i)n(i)} \\ &\geq \frac{1 + m(i)n(i).\frac{\alpha^{g(i)}-1}{120m(i)n(i)}}{\alpha^{g(i)}.120m(i)n(i)} = \frac{1}{120m(i)n(i)} \end{aligned}$$

which is evidently bigger than $log(|\ G\ |)^{-c}$ for sufficiently large i. Now let $f(i) > 0$. If the order of H is $120m(i)$ then since there are $n(i)$ linear characters $\sum_{\rho=linear} \sum_{h \neq e, h \in H} |$ $\chi_\rho(h) | \leq n(i)(120m(i) - 1)$. Also

$$|| H | [(\chi_\rho)_H, 1_H] - \chi_\rho(1) | \leq \chi_\rho(1)(120m(i) - 1)$$

$$\begin{aligned} (\mathbf{D}_H)\alpha^{g(i)}120m(i)n(i) \leq\ & n(i)(120m(i) - 1) + 2n(i)\frac{2(m(i) - 1)}{n(i)}2n(i)(120m(i) - 1) \\ & +3n(i)2(m(i) - 1)3n(i)(120m(i) - 1) \\ & +4n(i)2(m(i) - 1)4n(i)(120m(i) - 1) \\ & +5n(i)2(m(i) - 1)5n(i)(120m(i) - 1) \end{aligned}$$

$$+6n(i)2(m(i)-1)6n(i)(120m(i)-1).$$

Hence

$$\mathbf{D}_H < \frac{1}{\alpha^{g(n)}} + \frac{(8+18+16+25+36)m(i)n(i)}{\alpha^{g(i)}} < (log \mid G \mid)^{-c}$$

for each $c > 0$ and sufficiently large i. If order of H is $120n(i)$ then

$$\mid\mid H \mid [(\chi_\rho)_H, 1_H] - \chi_\rho(1) \mid \leq \chi_\rho(1)(120n(i)-1).$$

Since there are $n(i)$ linear characters the contribution from them is less than or equal to $n(i)(120n(i)-1)$. Then

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) \leq n(i)(120n(i)-1)$$

$$+2n(i)2(m(i)-1)2n(i)(120n(i)-1)$$

$$+3n(i)2(m(i)-1)3n(i)(120n(i)-1)$$

$$+4n(i)2(m(i)-1)4n(i)(120n(i)-1)$$

$$+5n(i)2(m(i)-1)5n(i)(120n(i)-1)$$

$$+6n(i)2(m(i)-1)6n(i)(120n(i)-1).$$

Hence

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) < 120(n(i)^3 + 8n(i)^3m(i) + 18n(i)^3m(i)$$

$$+32n(i)^3m(i) + 25n(i)^3m(i) + 36n(i)^3m(i))$$

$$< 120^2n(i)^3m(i).$$

Hence

$$\mathbf{D}_H < \frac{120n(i)^3m(i)}{\alpha^{g(i)}m(i)n(i)} < (log \mid G \mid)^{-c}$$

for each $c > 0$

and sufficiently large i from Lemma 3.7. If order of H is $m(i)$ then

$$|| H \mid [(\chi_\rho)_H, 1_H] - \chi_\rho(1) \mid \leq \chi_\rho(1)(m(i)-1).$$

The contribution from linear chararcters is less than or equal to $n(i)(m(i)-1)$. Thus

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) \leq n(i)(m(i)-1)$$

$$+2n(i)2(m(i)-1)2n(i)(m(i)-1)$$

$$+3n(i)2(m(i)-1)3n(i)(m(i)-1)$$

$$+4n(i)2(m(i)-1)4n(i)(m(i)-1)$$

$$+5n(i)(m(i)-1)5n(i)(m(i)-1)$$

$$+6n(i)(m(i)-1)6n(i)(m(i)-1)$$

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) < n(i)m(i) + 8m(i)^2n(i)^2 + 18m(i)^2n(i)^2$$

$$+32m(i)^2n(i)^2 + 25m(i)^2n(i)^2 + 36m(i)^2n(i)^2$$

Hence

$$\mathbf{D}_H < \frac{1}{120\alpha^{g(i)}} + \frac{119m(i)n(i)}{120\alpha^{g(i)}} < (log \mid G \mid)^{-c}$$

for each $c > 0$ and sufficiently large i from Lemma 3.7. If order of H is

$n(i)$ then the contribution from linear characters is less than or equal to $2(n(i)-1)$.

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) \leq 2(n(i)-1)$$

$$+2n(i)2(m(i)-1)2n(i)(n(i)-1)$$

$$+3n(i)2(m(i)-1)3n(i)(n(i)-1)$$

$$+4n(i)2(m(i)-1)4n(i)(n(i)-1)$$

$$+5n(i)2(m(i)-1)5n(i)(n(i)-1)$$

$$+6n(i)2(m(i)-1)6n(i)(n(i)-1).$$

Hence

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) < (n(i)^3 + 8n(i)^3m(i) + 18n(i)^3m(i)$$

$$+32n(i)^3m(i) + 25n(i)^3m(i) + 36n(i)^3m(i))$$

$$< 120n(i)^3m(i).$$

Hence

$$\mathbf{D}_H < \frac{n(i)^3m(i)}{\alpha^{g(i)}m(i)n(i)} < (log \mid G \mid)^{-c}$$

for each $c > 0$

and sufficiently large i from Lemma 3.7.

If the order of H is $m(i)n(i)$ then

$$\mid\mid H \mid [(\chi_\rho)_H, 1_H] - \chi_\rho(1) \mid \leq \chi_\rho(1)(m(i)n(i) - 1).$$

So the contribution from linear characters is less than or equal to $n(i)(m(i)n(i) - 1)$.

$$(\mathbf{D}_H)120\alpha^{g(i)}m(i)n(i) \leq n(i)(m(i)n(i) - 1)$$

$$+2n(i)2(m(i)n(i) - 1)2n(i)$$

$$+3n(i)2(m(i)n(i) - 1)3n(i)$$

$$+4n(i)2(m(i)n(i) - 1)4n(i)$$

$$+5n(i)(m(i)n(i) - 1)5n(i) + 6n(i)(m(i)n(i) - 1)6n(i)$$

Hence

$$\mathbf{D}_H < \frac{n(i)^2}{\alpha^{g(i)}} < (log \mid G \mid)^{-c}$$

for each $c > 0$ and

sufficiently large i from Lemma 3.7. Hence in all these cases H is indistinguishable.

Hence the proof. □

CHAPTER 4
ALGORITHMIC DISTINGUISHABILITY

In Chapter 3 we have discussed in detail Kempe-Shalev distinguishability as defined by Kempe and Shalev in (18). While the Kempe Shalev definition captures the difficulty of distinguishing the hidden subgroup from the trivial group in some cases, it is not always obvious how to translate its answers to practical algorithms. In this chapter we define "Algorithmic distinguishability". Algorithmic distinguishability defines distinguishability of a subgroup H of any finite group G from the trivial one on the basis of when a natural algorithm that uses the weak standard method succeeds in polynomial time. We study this new definition as applied to a number of examples. We also show that the new concept coincides for the Frobenius groups with the Kempe Shalev definition discussed in the previous chapter.

4.1 An algorithm for distinguishability

A natural algorithm to tell whether or not the hidden subgroup is trivial is as follows. Apply Quantum Fourier Sampling m times. Consider the resulting sequence of representations $\rho_1, .., \rho_m$. Ask whether it is more likely to obtain this particular sequence if the hidden subgroup is H or if it is trivial. Return 1 if it is H and return 0 if it is trivial. This algorithm is given by a function

$$\triangle : Irr(G)^m \to \{0, 1\}$$

which can be obtained as follows:

Let G be a finite group, and let H be a non-trivial subgroup of G. We denote

$$P_{H,1} : \mathrm{Irr}(G) \to [0, 1]$$

the function defined by

$$P_{H,1}(\chi) = \frac{\chi(1)|H|}{|G|}|\chi_H, 1_h|,$$

for all $\chi \in \mathrm{Irr}(G)$. For each positive integer m, we denote by

$$P_{H,m} : \mathrm{Irr}(G)^m \to [0,1]$$

the function defined by

$$P_{H,m}(\chi_1, \dots, \chi_m) = \prod_{i=1}^{m} P_{H,1}(\chi_i).$$

If m is understood from the context, we denote $P_{H,m}$ simply P_H. Let

$$\triangle : \mathrm{Irr}(G)^m \to \{0,1\}$$

be a function defined by

$$\triangle(\chi_1, .., \chi_m) = \begin{cases} 0 & P_{1,m}(\chi_1, .., \chi_m) \geq P_{H,m}(\chi_1, .., \chi_m) \\ 1 & P_{1,m}(\chi_1, .., \chi_m) < P_{H,m}(\chi_1, .., \chi_m) \end{cases}$$

Thus the formal algorithm is as follows:

Algorithm:

Step I: Repeat Quantum Fourier Sampling m times.

Step II: Get a sequence of ρ_i where $1 \leq i \leq m$.

Step III: Apply the function $\triangle$ to the tuple $(\rho_1, .., \rho_m)$.

Step IV: If the function returns 1 then H is non-trivial and if it returns 0 then otherwise.

Definition 6. Let G be a finite group, let H be a non-trivial subgroup of G, and let A and b be constants. We say that H is *distinguishable with constants* A and $b > 0$ if there exists some m such that the following hold.

1. $m \leq A \log_2(|G|)^b$
2. $$\sum_{(\chi_1,\dots,\chi_m) \in \triangle^{-1}(0)} P_1(\chi_1, \dots, \chi_m) > 1/2,$$

3. We also have the following:

$$\sum_{(\chi_1,\ldots,\chi_m)\in\triangle^{-1}(1)} P_H(\chi_1,\ldots,\chi_m) > 1/2.$$

Hence, we are saying that there is an algorithm f which given a sequence of results returns its guess of either *trivial* or *non trivial*, and this function is correct with more than probability $1/2$ both when the hidden subgroup is H and when the hidden subgroup is 1. This definition seems to capture the essence of what it means for a subgroup to be *distinguishable*. Most authors on Quantum Computing think in terms of sequences of groups, and for this reason the constants A and b need not be explicitly mentioned.

Definition 7. Let $(G_i)_{i=1}^{\infty}$ be a sequence of finite groups and let $(H_i)_{i=1}^{\infty}$ be a sequence of non-trivial subgroups where $H_i \leq G_i$. We say that $(H_i)_{i=1}^{\infty}$ is distinguishable if there exists some constants A and b, such that H_i is distinguishable with constants A and b in the previous sense for all i.

4.2 Abelian Groups

Using this definition we will first show that the non-trivial subgroups of an abelian group G are all algorithmically distinguishable.

Theorem 4.1. *All non-trivial subgroups H of an abelian group G are algorithmically distinguishable.*

Proof. Let G be an abelian group and H any non-trivial subgroup of G. Since G is abelian all irreducible characters of G are linear. H is normal in G and is contained in the kernels of $|G/H|$ linear characters. Now

$$P_H(\chi) = \frac{\chi(1)|H|<\chi_H, 1_H>}{|G|} = \begin{cases} 0 & H \nsubseteq ker(\chi) \\ \frac{1}{[G:H]} & otherwise \end{cases}$$

So

$$P_{H,m}(\chi_1,..,\chi_m) = \begin{cases} 0 & H \nsubseteq ker(\chi_i) \quad for \quad some \quad i \\ (\frac{1}{[G:H]})^m & otherwise \end{cases}$$

Also

$$P_{1,m}(\chi_1, .., \chi_m) = \prod_{i=1}^{m} \frac{1}{|G|} = (\frac{1}{|G|})^m.$$

We set

$$\triangle(\chi_1, .., \chi_m) = \begin{cases} 0 & P_{1,m}(\chi_1, .., \chi_m) > P_{H,m}(\chi_1, .., \chi_m) \\ 1 & P_{1,m}(\chi_1, .., \chi_m) < P_{H,m}(\chi_1, .., \chi_m) \end{cases}$$

We observe that

$$\sum_{(\chi_1,..,\chi_m)\in\triangle^{-1}(1)} P_{1,m}(\chi_1, .., \chi_m) = (\frac{1}{|G|})^m[(|G/H|)^m] = (\frac{1}{|H|})^m < 1/2$$

for all $m > 0$.

Hence

$$\sum_{(\chi_1,..,\chi_m)\in\triangle^{-1}(0)} P_{1,m}(\chi_1, .., \chi_m) > 1/2$$

for all $m > 0$.

Also

$$\sum_{(\chi_1,..,\chi_m)\in\triangle^{-1}(1)} P_{H,m}(\chi_1, .., \chi_m) = 1$$

for all $m > 0$. So H is distinguishable.

□

4.3 Frobenius Groups

In this section we study the algorithmic ditinguishability of the kernels and complements of the Frobenius groups discussed in Chapter 3. We have the following lemma.

Lemma 4.2. *If* $0 < x < 1$ *and* $k > 1$ *then*

$$(1 - x)^k > 1 - kx.$$

Proof. Let $f(x) = (1 - x)^k - (1 - kx)$. Differentiating both sides with respect to x we get

$$g(x) = -k(1 - x)^{k-1} + k = k[1 - (1 - x)^{k-1}] > 0.$$

Hence $f(x)$ is increasing and also $f(0) = 0$. Hence

$$(1-x)^k > 1 - kx.$$

□

Theorem 4.3. *Let $G = Z_{\alpha(\beta)}^{g(\beta)} \rtimes Z_\beta$ be a Frobenius group where $\alpha(\beta), g(\beta)$ are functions of β and $\alpha(\beta)$ is coprime to β and $\alpha(\beta), g(\beta) \to \infty$ as $\beta \to \infty$. Then the Kernel of G is algorithmically distinguishable and the complement is not.*

Proof. Let H be the kernel of G. Then H has order $\alpha(\beta)^{g(\beta)}$. Then

$$P_H(\chi) = \frac{\chi(1)|H|}{|G|} = \frac{\chi(1)\alpha(\beta)^{g(\beta)}}{\alpha(\beta)^{g(\beta)}\beta} = \frac{\chi(1)}{\beta}$$

if $H \subseteq ker(\chi)$ and is equal to 0 otherwise. Since H is in the kernel of only linear characters we have

$$P_H(\chi) = \frac{1}{\beta}$$

when $H \subseteq ker(\chi)$ and is equal to 0 otherwise. So

$$P_{H,m}(\chi_1, .., \chi_m) = \begin{cases} (\frac{1}{\beta})^m & \chi_i(1) = 1 \ \ and \ \ H \subseteq ker(\chi_i) \\ 0 & otherwise \end{cases}$$

Also

$$P_{1,m}(\chi_1, .., \chi_m) = \prod_{i=1}^{m} \frac{\chi_i(1)^2}{\alpha(\beta)^{g(\beta)}\beta}.$$

So we see that $P_{1,m}(\chi_1, .., \chi_m) > P_{H,m}(\chi_1, ..., \chi_m)$ if $P_{H,m}(\chi_1, .., \chi_m) = 0$. and $P_{1,m}(\chi_1, .., \chi_m) < P_{H,m}(\chi_1, ..., \chi_m)$ otherwise. We set

$$\triangle(\chi_1, .., \chi_m) = \begin{cases} 1 & P_{H,m}(\chi_1, .., \chi_m) > P_{1,m}(\chi_1, .., \chi_m) \\ 0 & P_{H,m}(\chi_1, .., \chi_m) < P_{1,m}(\chi_1, .., \chi_m) \end{cases}$$

Now

$$\sum_{(\chi_1,..,\chi_m) \in \triangle^{-1}(1)} P_{1,m}(\chi_1, .., \chi_m) = (\frac{1}{\alpha(\beta)^{g(\beta)}\beta})^m \beta^m < 1/2.$$

Hence

$$\sum_{(\chi_1,..,\chi_m)\in\triangle^{-1}(0)} P_{1,m}(\chi_1,..,\chi_m) > 1/2$$

for all $m > 0$ and $\beta \to \infty$.

Also

$$\sum_{(\chi_1,..,\chi_m)\in\triangle^{-1}(1)} P_{H,m}(\chi_1,..,\chi_m) = 1.$$

Hence H is algorithmically distinguishable.

Let H now be the Frobenius complement. Then $|H| = \beta$ and

$$P_H(\chi) = \frac{\chi(1)|H|}{|G|} < \chi_H, 1_H >= \begin{cases} \frac{|H|}{|G|} & \chi = 1_G \\ \frac{\chi(1)^2}{|G|} & \chi(1) = \beta \\ 0 & otherwise \end{cases}$$

$$= \begin{cases} \frac{1}{\alpha^{g(\beta)}} & \chi = 1_G \\ \frac{\beta}{\alpha^{g(\beta)}} & \chi(1) = \beta \\ 0 & otherwise \end{cases}$$

$$= \begin{cases} \frac{\chi(1)}{\alpha^{g(\beta)}} & \chi = 1_G \quad \chi(1) = \beta \\ 0 & otherwise. \end{cases}$$

So

$$P_{H,k}(\chi_1,..,\chi_k) = \begin{cases} \prod_{i=1}^{k} \frac{\chi_i(1)}{\alpha^{g(\beta)}} & \chi_i = 1_G \quad \chi_i(1) = \beta \\ 0 & otherwise \end{cases}$$

Also

$$P_{1,k}(\chi_1,..,\chi_k) = \prod_{i=1}^{k} \frac{\chi_i(1)^2}{\alpha^{g(\beta)}\beta}$$

Set

$$\triangle(\chi_1,..,\chi_k) = \begin{cases} 0 & P_{1,k}(\chi_1,..,\chi_k) = P_{H,k}(\chi_1,..,\chi_k) \\ 0 & P_{1,k}(\chi_1,..,\chi_k) > P_{H,k}(\chi_1,..,\chi_k) \\ 1 & P_{1,k}(\chi_1,..,\chi_k) < P_{H,k}(\chi_1,..,\chi_k) \end{cases}$$

We notice that

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} P_{H,k}(\chi_1,..,\chi_k) = \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} \prod_{i=1}^{k} \frac{\chi_i(1)}{\alpha^{g(\beta)}}$$

$$= \frac{1}{(\alpha^{g(\beta)})^k}[(1+(\alpha^{g(\beta)}-1))^k - (\alpha^{g(\beta)}-1)^k] = [1-(1-\frac{1}{\alpha^{g(\beta)}})^k].$$

Now since $k < c\lg(|G|)^b$ where $c > 0$ and $b > 0$, for large β, we have

$$\frac{k}{\alpha(\beta)^{g(\beta)}} < 1/2.$$

By the previous Lemma we get

$$(1-\frac{1}{\alpha^{g(\beta)}})^k > 1 - \binom{k}{1}\frac{1}{\alpha(\beta)^{g(\beta)}} > 1/2.$$

This in turn implies that

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} P_{H,k}(\chi_1,..,\chi_k) < 1/2.$$

Hence H is not algorithmically distinguishable.

□

Corollary 4.4. *Let $G = Z_p \rtimes Z_2$ be a Frobenius group. The kernel of G is algorithmically distinguishable and the complement is not.*

Corollary 4.5. *Let $G = Z_2^{p-1} \rtimes Z_p$ be a Frobenius group. The kernel of G is algorithmically distinguishable and the complement is not.*

Theorem 4.6. *Let $G = Z_\alpha^{g(i)} \rtimes Z_{m(i)} \rtimes Z_{n(i)}$ be a Frobenius group where $(m(i), n(i)) = 1$ and α is coprime to $m(i)$ and $n(i)$. We also assume $m(i)$, $n(i)$, $g(i) \to \infty$ as $i \to \infty$. Then the kernel of G is algorithmically distinguishable but the complement is not.*

Proof. If $G = Z_\alpha^{g(i)} \rtimes Z_{m(i)} \rtimes Z_{n(i)}$ and $|H| = \alpha^{g(i)}$. Now

$$P_H(\chi) = \frac{\chi(1)|H|}{|G|} < \chi_H, 1_H > .$$

Also

$$P_1(\chi) = \frac{\chi(1)^2}{|G|}.$$

So

$$P_H(\chi) = \begin{cases} \frac{\chi(1)^2}{m(i)n(i)} & H \subseteq Ker(\chi) \\ 0 & otherwise \end{cases}$$

Hence

$$P_{H,m}(\chi_1, .., \chi_k) = \begin{cases} \prod_{i=1}^{k} \frac{\chi_i(1)^2}{m(i)n(i)} & H \subseteq Ker(\chi_i) \\ 0 & otherwise \end{cases}$$

Also

$$P_{1,k}(\chi_1, .., \chi_k) = \prod_{i=1}^{k} \frac{\chi_i(1)^2}{\alpha^{g(i)} m(i)n(i)}.$$

Set

$$\triangle(\chi_1, .., \chi_k) = \begin{cases} 0 & P_{1,k}(\chi_1, .., \chi_k) > P_{H,m}(\chi_1, .., \chi_k) \\ 1 & P_{1,k}(\chi_1, .., \chi_k) < P_{H,m}(\chi_1, .., \chi_k) \end{cases}$$

So

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(0)} P_{1,k}(\chi_1, .., \chi_k) = \frac{1}{(\alpha^{g(i)} m(i)n(i))^k} \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(0)} \prod_{i=1}^{k} \chi_i(1)^2$$

$$\geq \frac{1}{(\alpha^{g(i)} m(i)n(i))^k} \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(0)} m(i)^{2k} n(i)^{2k} = \frac{m(i)^k n(i)^k}{\alpha^{g(i)k}} \frac{(\alpha^{g(i)} - 1)^k}{m(i)^k n(i)^k}$$

$$= (1 - \frac{1}{\alpha^{g(i)}})^k > 1/2$$

as $i \to \infty$. Also

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} P_{H,k}(\chi_1, .., \chi_k) > 1/2.$$

Hence H is distinguishable.

If $|H| = m(i)n(i)$ then

$$P_H(\chi) = \frac{\chi(1)|H|}{|G|} < \chi_H, 1_H >= \begin{cases} \frac{|H|}{|G|} & \chi = 1_G \\ \frac{\chi(1)^2}{|G|} & \chi(1) = m(i)n(i) \\ 0 & otherwise \end{cases}$$

$$= \begin{cases} \frac{1}{\alpha^{g(i)}} & \chi = 1_G \\ \frac{m(i)n(i)}{\alpha^{g(i)}} & \chi(1) = m(i)n(i) \\ 0 & otherwise \end{cases}$$

$$= \begin{cases} \frac{\chi(1)}{\alpha^{g(i)}} & \chi = 1_G \quad \chi(1) = m(i)n(i) \\ 0 & otherwise. \end{cases}$$

So

$$P_{H,k}(\chi_1, .., \chi_k) = \begin{cases} \prod_{i=1}^{k} \frac{\chi(1)}{\alpha^{g(i)}} & \chi = 1_G \quad \chi(1) = m(i)n(i) \\ 0 & otherwise \end{cases}$$

Also

$$P_{1,k}(\chi_1, .., \chi_k) = \prod_{i=1}^{k} \frac{\chi(1)^2}{\alpha^{g(i)} m(i)n(i)}$$

Set

$$\triangle(\chi_1, .., \chi_k) = \begin{cases} 0 & P_{1,k}(\chi_1, .., \chi_k) = P_{H,k}(\chi_1, .., \chi_k) \\ 0 & P_{1,k}(\chi_1, .., \chi_k) > P_{H,k}(\chi_1, .., \chi_k) \\ 1 & P_{1,k}(\chi_1, .., \chi_k) < P_{H,k}(\chi_1, .., \chi_k) \end{cases}$$

We notice that

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} P_{H,k}(\chi_1, .., \chi_k) = \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} \prod_{i=1}^{k} \frac{\chi_i(1)}{\alpha^{g(i)}}$$

$$= \frac{1}{(\alpha^{g(i)})^k}[(1 + (\alpha^{g(i)} - 1))^k - (\alpha^{g(i)} - 1)^k] = [1 - (1 - \frac{1}{\alpha^{g(i)}})^k].$$

The above expression is less than $1/2$ for $i \to \infty$ and small k. So H is not algorithmically distinguishable.

□

Theorem 4.7. *Let $G = Z_\alpha^{g(i)} \rtimes (SL(2,5) \times Z_{m(i)} \rtimes Z_{n(i)})$ be a Frobenius group where $i \in N$, $(m(i), n(i)) = 1$ and $\alpha > 1$ is a constant and coprime to $m(i)$, $n(i)$. We also assume that $m(i), n(i), g(i) \to \infty$ as $i \to \infty$. Then the kernel of this Frobenius group is algorithmically distinguishable but the complement is not.*

Proof. Let H be the Frobenius kernel. So $|H| = \alpha^{g(i)}$. Now

$$P_H(\chi) = \frac{\chi(1)|H|}{|G|} < \chi_H, 1_H > .$$

Also

$$P_1(\chi) = \frac{\chi(1)^2}{|G|}.$$

So

$$P_H(\chi) = \begin{cases} \frac{\chi(1)^2}{120m(i)n(i)} & H \subseteq Ker(\chi) \\ 0 & otherwise \end{cases}$$

So

$$P_{H,m}(\chi_1, .., \chi_k) = \begin{cases} \prod_{i=1}^{k} \frac{\chi_i(1)^2}{120m(i)n(i)} & H \subseteq Ker(\chi_i) \\ 0 & otherwise \end{cases}$$

Also

$$P_{1,k}(\chi_1, .., \chi_k) = \prod_{i=1}^{k} \frac{\chi_i(1)^2}{120\alpha^{g(i)}m(i)n(i)}.$$

Set

$$\triangle(\chi_1, .., \chi_k) = \begin{cases} 0 & P_{1,k}(\chi_1, .., \chi_k) > P_{H,m}(\chi_1, .., \chi_k) \\ 1 & P_{1,k}(\chi_1, .., \chi_k) < P_{H,m}(\chi_1, .., \chi_k) \end{cases}$$

So

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(0)} P_{1,k}(\chi_1, .., \chi_k) = \frac{1}{(120\alpha^{g(i)}m(i)n(i))^k} \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(0)} \prod_{i=1}^{k} \chi_i(1)^2$$

$$\geq \frac{1}{(120\alpha^{g(i)}m(i)n(i))^k} \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(0)} m(i)^{2k}n(i)^{2k} = \frac{m(i)^k n(i)^k}{120^k\alpha^{g(i)k}} \frac{(\alpha^{g(i)}-1)^k}{120^k m(i)^k n(i)^k}$$

$$= (\frac{1}{120} - \frac{1}{120\alpha^{g(i)}})^k > 1/2$$

as $i \to \infty$. Also

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} P_{H,k}(\chi_1, .., \chi_k) > 1/2.$$

Hence H is algorithmically distinguishable.

If $|H| = 120m(i)n(i)$ then

$$P_H(\chi) = \frac{\chi(1)|H|}{|G|} < \chi_H, 1_H >= \begin{cases} \frac{|H|}{|G|} & \chi = 1_G \\ \frac{\chi(1)^2}{|G|} & \chi(1) = 120m(i)n(i) \\ 0 & otherwise \end{cases}$$

$$= \begin{cases} \frac{1}{\alpha^{g(i)}} & \chi = 1_G \\ \frac{120m(i)n(i)}{\alpha^{g(i)}} & \chi(1) = 120m(i)n(i) \\ 0 & otherwise \end{cases}$$

$$= \begin{cases} \frac{\chi(1)}{\alpha^{g(i)}} & \chi = 1_G \quad \chi(1) = 120m(i)n(i) \\ 0 & otherwise. \end{cases}$$

So

$$P_{H,k}(\chi_1, .., \chi_k) = \begin{cases} \prod_{i=1}^{k} \frac{\chi(1)}{\alpha^{g(i)}} & \chi = 1_G \quad \chi(1) = 120m(i)n(i) \\ 0 & otherwise \end{cases}$$

Also

$$P_{1,k}(\chi_1, .., \chi_k) = \prod_{i=1}^{k} \frac{\chi(1)^2}{120\alpha^{g(i)}m(i)n(i)}$$

Set

$$\triangle(\chi_1, .., \chi_k) = \begin{cases} 0 & P_{1,k}(\chi_1, .., \chi_k) = P_{H,k}(\chi_1, .., \chi_k) \\ 0 & P_{1,k}(\chi_1, .., \chi_k) > P_{H,k}(\chi_1, .., \chi_k) \\ 1 & P_{1,k}(\chi_1, .., \chi_k) < P_{H,k}(\chi_1, .., \chi_k) \end{cases}$$

We notice that

$$\sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} P_{H,k}(\chi_1, .., \chi_k) = \sum_{(\chi_1,..,\chi_k)\in\triangle^{-1}(1)} \prod_{i=1}^{k} \frac{\chi_i(1)}{\alpha^{g(i)}}$$

$$= \frac{1}{(\alpha^{g(i)})^k}[(1 + (\alpha^{g(i)} - 1))^k - (\alpha^{g(i)} - 1)^k] = [1 - (1 - \frac{1}{\alpha^{g(i)}})^k].$$

This expression is less than $1/2$ for $i \to \infty$ and small k. Hence H is not algorithmically distinguishable. □

We note that in all the cases we have looked at so far, Kempe-Shalev distinguishability coincides with Algorithmic distinguishability.

CHAPTER 5
SOME CALCULATIONS

Even though Kempe-Shalev distinguishability and Algorithmic distinguishability coincide in the cases described in Chapter 3 and Chapter 4 these two concepts appear to be different. The following is an example where they seem not to coincide.

Here we pick some positive integer n and set $G = S_3 \times ... \times S_3$, where S_3 is the symmetric group on three letters and there are exactly n copies of it in the product. We fix t to be an element of order 3 in S_3 and we let H be the subgroup of G generated by $(t, t, ..., t)$. Then H has order 3.

Now $Irr(S_3) = \{1_{S_3}, sgn, \psi\}$, where 1_{S_3} is the principal character,sgn is the sign character, and ψ is the unique non-linear character. Both 1_{S_3} and sgn are linear, and $\psi(1) = 2$. Furthermore, we notice that the values of these characters on t are as follows. Both linear characters have value 1 on t, and $\psi(t) = -1$. Now $Irr(G)$ can be thought of as the cartesian product of n copies of $Irr(S_3)$. Hence $|Irr(G)| = 3^n$, and the degrees of these irreducible characters are of the form 2^i for some i with $0 \leq i \leq n$. Any character of degree 2^i can be obtained uniquely by choosing i locations out of n (where the character will be taken to be ψ) and then choosing one or other of the linear characters for all the other locations. Hence, there are exactly $\binom{n}{i}2^{n-i}$ characters in $Irr(G)$ of degree 2^i.

5.1 Kempe-Shalev distinguishability

Using the definition of Kempe-Shalev distinguishability we see that

$$D_H = \frac{1}{6^n}\sum_{\rho} d_\rho |\sum_{h\neq e} \chi_\rho(h)| =$$

$$\frac{1}{6^n}[\sum_{\rho} d_{\rho=linear}|\sum_{h\neq e}\chi_\rho(h)| + \sum_{\rho=non-linear} d_\rho|\sum_{h\neq e}\chi_\rho(h)|] =$$

$$\frac{1}{6^n}[2^n 2 + 2(|-1-1|\binom{n}{1}2^{n-1}) + 4(|1+1|\binom{n}{2}2^{n-2}) + .. + 2^n\binom{n}{n}] =$$

$$\frac{1}{6^n}[2^{n+1} + 2^{n+1}[\binom{n}{1} + ... + \binom{n}{n}]] = \frac{1}{6^n}[2^{n+1}(1+(2^n-1))] = \frac{2^{n+1}2^n}{6^n} = (\frac{2}{3})^n 2 < (n\log(6))^{-c}$$

for all $c > 0$ as $n \to \infty$.

Hence H is Kempe-Shalev indistinguishable.

5.2 Algorithmic Distinguishability

Let $\chi \in Irr(G)$ have $\chi(1) = 2^i$. Then $\chi((t, t, .., t)) = (-1)^i$. It follows that

$$P_{H,1}(\chi) = \frac{2^i 3}{6^n}\frac{1}{3}(2^i + 2(-1)^i).$$

Furthermore, we have

$$P_{1,1}(\chi) = \frac{\chi(1)}{6^n} < \chi_1, 1_1 >= \frac{\chi(1)^2}{6^n}.$$

Fix some positive integer m. The above computation yields that, for every $(\chi_1, .., \chi_m) \in Irr(G)^m$, we have

$$P_{H,m}(\chi_1, .., \chi_m) = \prod_{i=0}^{m} \frac{2^{\alpha_i}}{6^n}(2^{\alpha_i} + 2(-1)^{\alpha_i}),$$

and

$$P_{1,m}(\chi_1, .., \chi_m) = \prod_{i=0}^{m} \frac{2^{2\alpha_i}}{6^n}.$$

for $i = 1, .., m$. It then follows that

$$P_{H,m}(\chi_1, .., \chi_m) = P_{1,m}(\chi_1, .., \chi_m) \prod_{i=0}^{m}(1 + \frac{(-1)^{\alpha_i}}{2^{\alpha_i - 1}}).$$

In view of these calculations, it is natural to define a function

$$\triangle : Irr(G)^m \to \{0, 1\}$$

by for $(\chi_1, .., \chi_m) \in Irr(G)$, we set

$$\triangle(\chi_1, .., \chi_m) = \begin{cases} 0 & P_{1,m}(\chi_1, .., \chi_m) = P_{H,m}(\chi_1, .., \chi_m) \\ 0 & P_{1,m}(\chi_1, .., \chi_k) > P_{H,k}(\chi_1, .., \chi_m) \\ 1 & P_{1,m}(\chi_1, .., \chi_k) < P_{H,k}(\chi_1, .., \chi_m) \end{cases}$$

Using this function f, the probability of it giving the correct answer when the hidden subgroup is 1 is

$$\sum_{(\chi_1, .., \chi_m) \in \triangle^{-1}(0)} P_1(\chi_1, .., \chi_m)$$

and the probability of it giving the correct answer when the hidden subgroup is H is

$$\sum_{(\chi_1,..,\chi_m)\in\triangle^{-1}(1)} P_H(\chi_1,..,\chi_m).$$

These numbers can be computed for small values of n and m using *GAP*. Here is a *GAP* program that calculates these probabilities.

```
C_1:=function(n,m)
local prob, tuples,reltuples, pp, a,s;
prob:=0;  reltuples:=[];
tuples:=Tuples([0..n],m);
for a in tuples do
pp:=Product(a, x -> (1 + (-1)^x/(2^(x-1))));
if pp <= 1 then Append(reltuples,[a]);fi;
od;
for a in reltuples do
s:=Product(a, x -> Binomial(n,x));
s:= s*Product(a, x -> 2^(n - x));
s:= s*Product(a, x -> 2^(2*x)/(6^n));
prob:=prob + s;
od;
return prob;
end;
C_2:=function(n,m)
local prob, tuples,reltuples, pp, a,s;
prob:=0;  reltuples:=[];
tuples:=Tuples([0..n],m);
for a in tuples do
pp:=Product(a, x -> (1 + (-1)^x/(2^(x-1))));
```

```
if pp > 1 then Append(reltuples,[a]);fi;
od;
for a in reltuples do
s:=Product(a, x -> Binomial(n,x));
s:= s*Product(a, x -> 2^(n - x));
s:= s*Product(a, x -> 2^(x) *(2^x + 2*(-1)^x)/(6^n));
prob:=prob + s;
od;
return prob;
end;
```

The computation appears to show that the subgroup H is distinguishable according to our definition in the cases we tried. For some computations see charts in appendix B.

APPENDIX A
TABLES FOR CHAPTER 4

Here are the tables for Chapter 4.

Table A-1.

$H = SY_1$						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$\frac{1}{3^i}$	0	0	0	0	0
Z_0	1-$\frac{1}{3^i}$	1	0	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{3^i}$
SY_1	0	0	1	0	0	0
SY_2	0	0	0	$\frac{1}{2^i}$	0	0
SY_3	0	0	0	0	$\frac{1}{2^i}$	0
$H_t(k)$	0	0	0	0	0	0
$H(k)$	0	0	0	0	0	0
G	0	0	0	0	0	$\frac{1}{3^i}$

Table A-2.

$H = SY_1$ Intermediate						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$1 - \frac{1}{3^i}$	1	1	1	1	1-$\frac{1}{3^i}$
Z_0	0	0	0	0	0	0
SY_1	1-$\frac{1}{3^i}$	1	0	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{3^i}$
SY_2	1-$\frac{1}{3^i}$	1	0	$1 - \frac{1}{2^i}$	$1 - \frac{1}{2^i}$	$1 - \frac{1}{3^i}$
SY_3	1-$\frac{1}{3^i}$	1	0	$1 - \frac{1}{2^i}$	$1 - \frac{1}{2^i}$	$1 - \frac{1}{3^i}$
$H_t(k)$	0	0	0	0	0	0
$H(k)$	0	0	0	0	0	0
G	1	1	1	1	1	$1 - \frac{1}{3^i}$

Table A-3.

$H = SY_1$ Final	
	$H = SY_1$
TZ_0	$\frac{1}{3^i}(1-\frac{1}{3^i})$
Z_0	0
SY_1	$(1-\frac{1}{3^i})^2(1-\frac{1}{2^i}+\frac{1}{3.2^{2i}})$
SY_2	$\frac{1}{2}(1-\frac{1}{3^i})^2(1-\frac{1}{2^i})\frac{1}{2^i}+\frac{1}{3}(1-\frac{1}{3^i})^2\frac{1}{2^{2i}}$
SY_3	$\frac{1}{2}(1-\frac{1}{3^i})^2(1-\frac{1}{2^i})\frac{1}{2^i}+\frac{1}{3}(1-\frac{1}{3^i})^2\frac{1}{2^{2i}}$
$H_t(k)$	0
$H(k)$	0
G	$\frac{1}{3^i}$

Table A-4.

$H = TZ_0$						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	1	0	0	0	0	1-$\frac{1}{2^i}$
Z_0	0	1	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	0
SY_1	0	0	$\frac{1}{2^i}$	0	0	0
SY_2	0	0	0	$\frac{1}{2^i}$	0	0
SY_3	0	0	0	0	$\frac{1}{2^i}$	0
$H_t(k)$	0	0	0	0	0	0
$H(k)$	0	0	0	0	0	0
G	0	0	0	0	0	$\frac{1}{2^i}$

Table A-5.

$H = TZ_0$ Intermediate						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	0	1	1	1	1	0
Z_0	0	0	0	0	0	0
SY_1	0	1	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	0
SY_2	0	1	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	0
SY_3	0	1	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	0
$H_t(k)$	0	0	0	0	0	0
$H(k)$	0	0	0	0	0	0
G	1	1	1	1	1	$1-\frac{1}{2^i}$

Table A-6.

$H = TZ_0$ Final	
	$H = TZ_0$
TZ_0	$(1-\frac{1}{2^i})$
Z_0	0
SY_1	0
SY_2	0
SY_3	0
$H_t(k)$	0
$H(k)$	0
G	$\frac{1}{2^i}$

Table A-7.

$H = Z_0$						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$\frac{1}{3^i}$	0	0	0	0	$\frac{1}{3^i}$-$\frac{1}{6^i}$
Z_0	1-$\frac{1}{3^i}$	1	$1-\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{3^i}$
SY_1	0	0	$\frac{1}{2^i}$	0	0	0
SY_2	0	0	0	$\frac{1}{2^i}$	0	0
SY_3	0	0	0	0	$\frac{1}{2^i}$	0
$H_t(k)$	0	0	0	0	0	0
$H(k)$	0	0	0	0	0	0
G	0	0	0	0	0	$\frac{1}{6^i}$

Table A-8.

$H = Z_0$ Intermediate						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$1-\frac{1}{3^i}$	1	1	1	1	$1-\frac{1}{3^i}$
Z_0	0	0	0	0	0	0
SY_1	1-$\frac{1}{3^i}$	1	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{3^i}$
SY_2	1-$\frac{1}{3^i}$	1	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{3^i}$
SY_3	1-$\frac{1}{3^i}$	1	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{2^i}$	$1-\frac{1}{3^i}$
$H_t(k)$	0	0	0	0	0	0
$H(k)$	0	0	0	0	0	0
G	1	1	1	1	1	$1-\frac{1}{6^i}$

Table A-9.

Final Probabilities	
	$H = Z_0$
TZ_0	$\frac{1}{3^i}(2 - \frac{1}{2^i} - \frac{1}{3^i})$
Z_0	$(1 - \frac{1}{3^i})(1 - \frac{1}{2^i})^3(1 - \frac{1}{3^i})$
SY_1	$(1 - \frac{1}{3^i})^2(1 - \frac{1}{2^i})^2\frac{1}{2^i} + (1 - \frac{1}{3^i})^2(1 - \frac{1}{2^i})\frac{1}{2^{2i}} + \frac{1}{3}(1 - \frac{1}{3^i})^2\frac{1}{2^{3i}}$
SY_2	$(1 - \frac{1}{3^i})^2(1 - \frac{1}{2^i})^2\frac{1}{2^i} + (1 - \frac{1}{3^i})^2(1 - \frac{1}{2^i})\frac{1}{2^{2i}} + \frac{1}{3}(1 - \frac{1}{3^i})^2\frac{1}{2^{3i}}$
SY_3	$(1 - \frac{1}{3^i})^2(1 - \frac{1}{2^i})^2\frac{1}{2^i} + (1 - \frac{1}{3^i})^2(1 - \frac{1}{2^i})\frac{1}{2^{2i}} + \frac{1}{3}(1 - \frac{1}{3^i})^2\frac{1}{2^{3i}}$
$H_t(k)$	0
$H(k)$	0
G	$\frac{1}{6^i}$

Table A-10.

$H = H_t(k)$						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$(\frac{1}{2^{n-k-1}})^i$	0	0	0	0	$(\frac{1}{2^{n-k}})^i(2^i-1)$
Z_0	0	$(\frac{1}{2^{n-k-1}})^i$	$(\frac{1}{2^{n-k}})^i(2^i-1)$	$(\frac{1}{2^{n-k}})^i(2^i-1)$	$(\frac{1}{2^{n-k}})^i(2^i-1)$	0
SY_1	0	0	$(\frac{1}{2^{n-k}})^i$	0	0	0
SY_2	0	0	0	$(\frac{1}{2^{n-k}})^i$	0	0
SY_3	0	0	0	0	$(\frac{1}{2^{n-k}})^i$	0
$H_t(k)$	1-$\frac{1}{2^i}$	0	0	0	0	1-$\frac{1}{2^i}$
$H_t(m)$	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	0	0	0	0	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$
$H(m)$	0	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	0
$H(k)$	0	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	1-$\frac{1}{2^i}$	0
G	0	0	0	0	0	$(\frac{1}{2^{n-k}})^i$

Table A-11.

$H = H_t(k)$ Intermediate						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$1-(\frac{1}{2^{n-k-1}})^i$	1	1	1	1	$1-(\frac{1}{2^{n-k-1}})^i$
Z_0	$1-(\frac{1}{2^{n-k-2}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{1}{2^{n-k-2}})^i$
SY_1	$1-(\frac{1}{2^{n-k-1}})^i$	1	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$
SY_2	$1-(\frac{1}{2^{n-k-1}})^i$	1	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$
SY_3	$1-(\frac{1}{2^{n-k-1}})^i$	1	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$
$H_t(k)$	0	1-$\frac{1}{2^{2i}}$	1-$\frac{1}{2^{2i}}$	1-$\frac{1}{2^{2i}}$	1-$\frac{1}{2^{2i}}$	0
$H_t(m)$	$1-(\frac{1}{2^{m-k}})^i$	1-$(\frac{1}{2^{m-k+2}})^i$	1-$(\frac{1}{2^{m-k+2}})^i$	1-$(\frac{1}{2^{m-k+2}})^i$	1-$(\frac{1}{2^{m-k+2}})^i$	1-$(\frac{1}{2^{m-k}})^i$
$H(m)$	1-$(\frac{1}{2^{m-k-1}})^i$	$1-(\frac{1}{2^{m-k}})^i$	$1-(\frac{1}{2^{m-k}})^i$	1-$(\frac{1}{2^{m-k}})^i$	1-$(\frac{1}{2^{m-k}})^i$	1-$(\frac{1}{2^{m-k-1}})^i$
$H(k)$	0	0	0	0	0	0
G	1	1	1	1	1	1-$(\frac{1}{2^{n-k}})^i$

Table A-12.

Final probabilities	
	$H = H_t(k)$
Z_0	$(1-(\frac{1}{2^{n-k-2}})^i)^2(1-(\frac{1}{2^{n-k}})^i)^3-(1-(\frac{1}{2^{n-k-2}})^i)^2(1-(\frac{1}{2^{n-k-1}})^i)^4$
TZ_0	$(1-(\frac{1}{2^{n-k}})^i)-(1-(\frac{1}{2^{n-k-1}})^i)^2$
SY_1	$(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^i(1-(\frac{1}{2^{n-k}})^i)^2+(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^{2i}(1-(\frac{1}{2^{n-k}})^i)+\frac{1}{3}(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^{3i}$
SY_2	$(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^i(1-(\frac{1}{2^{n-k}})^i)^2+(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^{2i}(1-(\frac{1}{2^{n-k}})^i)+\frac{1}{3}(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^{3i}$
SY_3	$(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^i(1-(\frac{1}{2^{n-k}})^i)^2+(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^{2i}(1-(\frac{1}{2^{n-k}})^i)+\frac{1}{3}(1-(\frac{1}{2^{n-k-1}})^i)^2(\frac{1}{2^{n-k}})^{3i}$
$H_t(k)$	$(1-\frac{1}{2^i})^2(1-\frac{1}{2^{2i}})^4$
$H_t(m)$	$(1-(\frac{1}{2^{m-k+1}})^i)^2(1-(\frac{1}{2^{m+k+2}})^i)^4-(1-(\frac{1}{2^{m-k}})^i)^2(1-(\frac{1}{2^{m+k+2}})^i)^4$
$H(k)$	0
$H(m)$	$(1-(\frac{1}{2^{m-k-1}})^i)^2(1-(\frac{1}{2^{m-k+1}})^i)^5-(1-(\frac{1}{2^{m-k-1}})^i)^2(1-(\frac{1}{2^{m-k}})^i)^4$
G	$(\frac{1}{2^{n-k}})^i$

Table A-13.

$H = H(k)$						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	$\frac{1}{3^i}(\frac{1}{2^{n-k-1}})^i$	0	0	0	0	$(\frac{2^{k-n+1}}{3})^i - (\frac{2^{k-n}}{3})^i$
Z_0	$(1-\frac{1}{3^i})(\frac{1}{2^{n-k-1}})^i$	$(1/2^{n-k-1})^i$	$(\frac{1}{2^{n-k}})^i(2^i-1)$	$(\frac{1}{2^{n-k}})^i(2^i-1)$	$(\frac{1}{2^{n-k}})^i(2^i-1)$	$(2^{k-n+1})^i - (\frac{2^{k-n+1}}{3})^i$
SY_1	0	0	$(1/2^{n-k})^i$	0	0	0
SY_2	0	0	0	$(\frac{1}{2^{n-k}})^i$	0	0
SY_3	0	0	0	0	$(\frac{1}{2^{n-k}})^i$	0
$H_t(k)$	$\frac{1}{3^i}(1-\frac{1}{2^i})$	0	0	0	0	$\frac{1}{3^i}(1-(\frac{1}{2})^i$
$H_t(m)$	$\frac{1}{3^i}(2^i-1)(\frac{1}{2^{m-k+1}})^i$	0	0	0	0	$(\frac{2^{k-m}}{3})^i - (\frac{2^{k-m-1}}{3})^i$
$H(m)$	$(1-\frac{1}{3^i})(2^i-1)(\frac{1}{2^{m-k+1}})^i$	$\frac{1}{(2^{m-k})^i}(1-\frac{1}{2^i})$	$\frac{1}{(2^{m-k+1})^i}(2^i-1)$	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	$(\frac{1}{2^{m-k+1}})^i(2^i-1)$	$(2^{k-m-1})^i(1-\frac{1}{3^i})(2^i-1)$
$H(k)$	$(1-\frac{1}{3^i})(1-\frac{1}{2^i})$	$(1-\frac{1}{2^i})$	$(1-\frac{1}{2^i})$	$(1-\frac{1}{2^i})$	1-$\frac{1}{2^i}$	$(1-\frac{1}{3^i})(1-\frac{1}{2^i})$
G	0	0	0	0	0	$\frac{1}{3^i}(\frac{1}{2^{n-k}})^i$

Table A-14.

$H = H(k)$ Intermediate						
	TZ_0	Z_0	SY_1	SY_2	SY_3	G
TZ_0	1-$\frac{1}{3^i}(\frac{1}{2^{n-k-1}})^i$	1	1	1	1	$1-\frac{1}{3^i}(\frac{1}{2^{n-k-1}})^i$
Z_0	$1-\frac{1}{3^i}(\frac{1}{2^{n-k-2}})^i$	$1-(1/2^{n-k-1})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{1}{2^{n-k-1}})^i$	$1-(\frac{2^{k-n+2}}{3})^i$
SY_1	$1-\frac{1}{3^i}(\frac{1}{2^{n-k-1}})^i$	1	$1-(1/2^{n-k})^i$	$1-(1/2^{n-k})^i$	$1-(1/2^{n-k})^i$	$1-(\frac{1}{2^{n-k-2}})^i\frac{1}{3^i}$
SY_2	$1-\frac{1}{3^i}(\frac{1}{2^{n-k-1}})^i$	1	$1-(1/2^{n-k})^i$	$1-(1/2^{n-k})^i$	$1-(1/2^{n-k})^i$	$1-(\frac{1}{2^{n-k-2}})^i\frac{1}{3^i}$
SY_3	$1-\frac{1}{3^i}(\frac{1}{2^{n-k-1}})^i$	1	$1-(1/2^{n-k})^i$	$1-(1/2^{n-k})^i$	$1-(1/2^{n-k})^i$	$1-(\frac{1}{2^{n-k-2}})^i\frac{1}{3^i}$
$H_t(k)$	$(1-\frac{1}{3^i})(1-\frac{1}{2^{2i}})$	$1-\frac{1}{2^{2i}}$	$1-\frac{1}{2^{2i}}$	$1-\frac{1}{2^{2i}}$	$1-\frac{1}{2^{2i}}$	$(1-\frac{1}{2^{2i}})(1-\frac{1}{3^i})$
$H_t(m)$	$-\frac{1}{3^i}(\frac{1}{2^{m-k}})^i(1-\frac{1}{4^i}+\frac{3^i}{4^i})+1$	$1-(\frac{1}{2^{m-k+2}})^i)$	$1-(\frac{1}{2^{m-k+2}})^i)$	$1-(\frac{1}{2^{m-k+2}})^i)$	$1-(\frac{1}{2^{m-k+2}})^i)$	$-\frac{1}{3^i}(\frac{1}{2^{m-k}})^i(1-\frac{1}{4^i}+\frac{3^i}{4^i})+1$
$H(m)$	$\frac{1}{3^i}(1-(\frac{1}{2^{m-k-1}})^i)+(1-\frac{1}{3^i})(1-(\frac{1}{2^{m-k}})^i)$	$1-(\frac{1}{2^{m-k}})^i$	$1-(\frac{1}{2^{m-k}})^i$	$1-(\frac{1}{2^{m-k}})^i$	$1-(\frac{1}{2^{m-k}})^i$	$-(\frac{1}{2^{m-k}})^i(1+\frac{2^i}{3^i}-\frac{1}{3^i})+1$
$H(k)$	0	0	0	0	0	0
G	1	1	1	1	1	1-$\frac{1}{3^i}(\frac{1}{2^{n-k}})^i$

Table A-15.

Final	
	$H = H(k)$
Z_0	$(1-(\frac{2^{k-n+2}}{3})^i+(2^{k-n+1})^i-(\frac{2^{k-n+1}}{3})^i)^2-(1-(\frac{2^{k-n+2}}{3})^i)^2(1-(\frac{1}{2^{k-n+1}})^i)^4$
TZ_0	$(1-(\frac{2^{k-n}}{3})^i)-(1-(\frac{2^{k-n+1}}{3})^i)^2$
SY_1	$(1-(\frac{2^{k-n+1}}{3})^i)^2(\frac{1}{2^{n-k}})^i(1+(\frac{1}{2^{n-k}})^{2i}-(\frac{1}{2^{n-k}})^i)$
SY_2	$(1-(\frac{2^{k-n+1}}{3})^i)^2(\frac{1}{2^{n-k}})^i(1+(\frac{1}{2^{n-k}})^{2i}-(\frac{1}{2^{n-k}})^i)$
SY_3	$(1-(\frac{2^{k-n+1}}{3})^i)^2(\frac{1}{2^{n-k}})^i(1+(\frac{1}{2^{n-k}})^{2i}-(\frac{1}{2^{n-k}})^i)$
$H_t(k)$	$(1+\frac{1}{2^i}(\frac{1}{6^i}-\frac{1}{2^i}-\frac{1}{3^i}))^2(1-\frac{1}{2^{2i}})^4-(1-\frac{1}{3^i})^2(1-\frac{1}{2^{2i}})^6$
$H_t(m)$	$(1-(\frac{1}{2^{m-k+2}})^i)^4((1-(\frac{2^{k-m-1}}{3})^i+(\frac{2^{k-m-2}}{3})^i-(2^{k-m-2})^i)^2-(1-(\frac{2^{k-m}}{3})^i(1-\frac{1}{4^i}+\frac{3^i}{4^i}))^2)$
$H(k)$	$(1-\frac{1}{3^i})^2(1-\frac{1}{2^i})^6$
$H(m)$	$(1-(\frac{1}{2^{m-k-1}})^i-(\frac{2^{k-m+1}}{3})^i+(\frac{2^{k-m-1}}{3})^i)^2(1-(\frac{1}{2^{m-k+1}})^i)^4-(1-(\frac{1}{2^{m-k}})^i)^4(1-(\frac{1}{2^{m-k}})^i(1+\frac{2^i}{3^i}-\frac{1}{3^i}))^2$
G	$(\frac{1}{2^{n-k}})^i$

APPENDIX B
TABLE FOR CHAPTER 5

Table B-1. Table for $\sum P_{1,m}(\chi_1, .., \chi_m)$

C_1		
n	m	*sum*
4	3	$> 1/2$
5	4	$> 1/2$
6	5	$> 1/2$
7	6	$> 1/2$

Table B-2. Table for $\sum P_{H,m}(\chi_1, .., \chi_m)$

C_2		
n	m	*sum*
4	3	$> 1/2$
5	4	$> 1/2$
6	5	$> 1/2$
7	6	$> 1/2$

REFERENCES

[1] Dave Bacon, Andrew M. Childs, and Wim van Dam, *From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*, arXiv:quant-ph/0504083v2., 2005.

[2] R. Beals, *Quantum computation of fourier transforms over symmetric groups*, Proceedings of the twenty-ninth annual ACM symposium on Theory of computing. **29** (1997), 48–53.

[3] Ethan Bernstein and Umesh Vazirani, *Quantum complexity theory*, SIAM Journal on Computing **26(5)** (1997), 1411–1473.

[4] Thomas Beth, Markus Puschel, and Martin Rotteler, *Fast quantum fourier transforms for a class of non-abelian groups*, Lecture Notes In Computer Science. **1719** (1999), 148–159.

[5] Dong Pyo Chi, Jeong San Kim, and Soojoon Lee, *Notes on the hidden subgroup problem on some semi-direct product groups*, arXiv:quant-ph/0604172v1., 2006.

[6] David Deutsch, *Quantum computational networks*, Proceedings of the Royal Society of London A **425** (1989), 73–90.

[7] David Deutsch and Richard Jozsa, *Rapid solutions of problems by quantum computation*, Proceedings of the Royal Society of London A **439** (1992), 553–558.

[8] M. Ettinger and P. Hoyer, *On quantum algorithms for noncommutative hidden subgroups*, Adv. in Appl. Math **25(3)** (2000), 239–251.

[9] Richard P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics. **21:6/7** (1982), 467–488.

[10] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen, *Hidden translation and orbit coset in quantum computing*, Proceedings of 35th ACM Symposium on Theory of Computing **35** (2003), 1–9.

[11] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani, *Quantum mechanical algorithms for the nonabelian hidden subgroup problem*, Proc. Symp. Pure Math. **46** (1987), 111–138.

[12] S. Hallgren, A. Russell, and A. Ta-Shma, *The hidden subgroup problem and quantum computation using group representations*, Proceedings of 32th ACM Symposium on Theory of Computing. **32** (2000), 627–635.

[13] Mika Hirvensalo (ed.), *Quantum computing*, Springer., New York, 2001.

[14] Peter Hoyer, *Efficient quantum transforms*, quant-ph/9702028., 1997.

[15] Yoshifumi Inui and Francois Le Gall, *Efficient quantum algorithms for the hidden subgroup problem over a class of semi-direct product groups*, arXiv:quant-ph/0412033v3., 2004.

[16] I.M. Isaacs, *Character theory of finite groups*, Dover, New Yrok, 1994.

[17] G. Ivanyos, F. Magniez, and M. Santha, *Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem*, Proceedings of 13th ACM Symposium on Parallelism in Algorithms and Architectures. **13** (2001), 263–270.

[18] J. Kempe and A. Shalev, *The hidden subgroup problem and permutation group theory*, Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms . **16** (2005), 1118–1125.

[19] G. Kuperberg, *A subexponential-time algorithm for the dihedral hidden subgroup problem*, SIAM J. Comput. **35(1)** (2005), 170–188.

[20] Christopher Moore, Daniel Rockmore, and Alexander Russell, *Generic quantum ffts*, Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms. **15** (2004), 778–787.

[21] O. Regev, *A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space.*, http://xxx.lanl.gov/abs/quant-ph/0406151, 2004.

[22] J.P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

[23] P.W. Shor, *Algorithms for quantum computation: Discrete log and factoring*, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science . **35** (1994), 124–134.

[24] Daniel R. Simon, *On the power of quantum computation*, Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science **35** (1994), 116–123.

[25] Christof Zalka, *On a particular non-abelian hidden subgroup problem*, http://qso.lanl.gov/zalka/QC/QC.html, 1999.

BIOGRAPHICAL SKETCH

Anales Debhaumik was born in the year 1972 in Calcutta, India. He graduated with bachelor's in mathematics from Calcutta University. He also graduated with a master's degree in applied mathematics from Calcutta University and a master's degree in computer applications from Bangalore University, India. He came to United States in 2003 as a PhD student in mathematics Department of University of Florida. He received M.S in mathematics from University of Florida in the year 2005. He graduated with PhD in May 2010. His research interest is finite group theory.