Title
Implementing measurements and optimizing queries for the quantum hidden subgroup problem

Permalink
https://escholarship.org/uc/item/1325b186

Author
Shakeel, Asif

Publication Date
2011

Peer reviewed|Thesis/dissertation
Implementing Measurements and Optimizing Queries for the Quantum Hidden Subgroup Problem

A dissertation submitted in partial satisfaction of the requirements for the degree Doctor of Philosophy in Mathematics by Asif Shakeel

Committee in charge:

Professor David A. Meyer, Chair
Professor Nolan R. Wallach, Co-Chair
Professor Lu J. Sham
Professor Hans G. Wenzl
Professor Christian Wüthrich

2011
The dissertation of Asif Shakeel is approved, and it is acceptable in quality and form for publication on microfilm:

________________________________________

________________________________________

________________________________________

Co-Chair

Chair

University of California, San Diego

2011
# TABLE OF CONTENTS

## Signature Page

Signature Page ........................................ iii

## Table of Contents

Table of Contents ....................................... iv

## List of Figures

List of Figures .......................................... vi

## List of Tables

List of Tables .......................................... vii

## Acknowledgements

Acknowledgements ....................................... viii

## Vita and Publications

Vita and Publications ................................ x

## Abstract

Abstract ................................................ x

### Chapter 1. Introduction

1.1. Background ........................................ 1

1.2. The Hidden Subgroup Problem (HSP) ................ 7

1.3. Basic representation theory ..................... 9

1.3.1. Definitions .................................... 10

1.3.2. The group algebra $\mathbb{C}[G]$ ................ 11

1.3.3. The Fourier transform ......................... 13

1.3.4. Characters and projections .................... 14

1.3.5. Notation and frequently used results ........ 16

1.4. Summary of approaches and techniques .......... 17

1.4.1. Weak and strong Fourier sampling .......... 17

1.4.2. Subgroup reduction .......................... 18

1.4.3. Single-query vs multi-query .................. 18

1.4.4. The standard method in HSP ................. 19

1.4.5. State discrimination ......................... 20

### Chapter 2. PGM implementation for the Dihedral HSP

2.1. Introduction ...................................... 22

2.2. The standard method ............................ 23

2.3. The single-query PGM ........................... 25

2.4. The multi-query PGM ............................ 29

2.5. The standard algorithm ......................... 42

2.6. Single-query algorithm ........................ 55

2.7. Multi-query algorithm .......................... 56

2.8. Computational complexity ....................... 58

2.9. Conclusion and discussion ....................... 61
Chapter 3. Single-query optimization ........................................ 63
  3.1. Introduction .................................................................... 64
    3.1.1. The phase kickback trick ........................................ 64
    3.1.2. The HSP and state discrimination ............................. 67
    3.1.3. Query search ......................................................... 70
  3.2. Background ................................................................. 72
  3.3. Subgroup states ............................................................ 75
  3.4. The character query and optimal measurements ............... 83
  3.5. Success probability of the character query ....................... 87
  3.6. Conjugate subgroups ..................................................... 93
  3.7. Conclusion and discussion ............................................. 94

Chapter 4. Some ideas in multi-query optimization ................. 97
  4.1. Introduction ............................................................... 97
  4.2. Some analysis of unentangled queries ............................ 97
  4.3. Numerical results and inferences .................................. 102
    4.3.1. Unentangled parallel queries .................................. 102
    4.3.2. Entangled parallel queries ......................................... 103
    4.3.3. Sequential queries ............................................... 105
  4.4. Future direction .......................................................... 106

Appendix A. The left translation representation of the dihedral group . . . 111
LIST OF FIGURES

Figure 1.1. NAND gate .................................................. 4
Figure 1.2. Toffoli gate .................................................... 4
Figure 1.3. CNOT gate ..................................................... 5

Figure 2.1. Single-query algorithm implementation ............... 56
Figure 2.2. Multi-query algorithm implementation ............... 58

Figure 3.1. Oracle function $f$ factors ............................. 77
LIST OF TABLES

Table 4.1. Unentangled character queries ........................................... 103
Table 4.2. Entangled character queries ............................................ 104
ACKNOWLEDGEMENTS

I would like to express my gratitude to my thesis advisor, Professor David Meyer, for his unwavering support, kindness, generosity, commitment and encouragement. He embodies a rare mix of trust, friendship, bold questioning, and foresight that one aspires to. At every stage of this dissertation he has discussed ideas, given insights and interpretations, motivated and suggested directions and worked with me tirelessly to carry them further. His intellectual and mathematical rigor, breadth of work, and emphasis on learning as much as imparting accessibly the subtleties of a topic are nonpareil. One can not help but learn to think freely with him.

I am equally grateful to Professor Nolan Wallach, first and foremost for being a great teacher and a very caring person to whom I could always talk with humor. From my introduction to abstract algebra to the understanding of representation theory and beyond, indeed that of quantum computation and hidden subgroup problem, all owe tremendously to my interactions with him, to his classes and also to reading his books and papers. I have turned to him and been guided by his vast and deep knowledge, wisdom of his advice, his sense of curiosity and urgency, and his ability to reach the very heart of a problem. He leads by example and much of the formulation in this dissertation has been influenced by his work.

I would also like to thank the rest of my thesis committee members Professors Lu Sham, Hans Wenzl and Christian Wüthrich for kindly accepting to be on the committee and giving their time and being open and available to discuss various aspects of the subject.

Thanks in no small part to Professor James Pommersheim, Dr. Orest Bucicovschi, Dr. Jiri Lebl, Dr. Jon Grice, and Professor Nitya Kitchloo for enlightening discussions and exchanges of ideas. Among other colleagues from the quantum computation and information research group, Thomas Wong, Daniel Minsky, and Benjamin Wilson, have contributed to making my ideas clearer in form and presentation. Thanks to Karl Fredrickson for interesting conversations and hikes.

Special thanks to Lois Stewart, Joyce Cheng, Sabrina Leitner and Kimberly Eaton of the UCSD mathematics department for keeping me aware and helping
me a lot with the procedural matters and for their kind words. Another thanks to the staff of computing support group, particularly Saul Molina and Wilson Cheung for their help in making my presentations possible. I would like to thank too the general faculty, administration and student body of the mathematics department for creating an excellent environment.

Finally, I would like to thank the dear people in my life and friends I have made over the course of last several years who kept my spirits up and made things fun.

Chapter 3, in part, has been submitted for publication of the material as *An improved query for the Hidden Subgroup Problem*, by A. Shakeel. The dissertation author was the primary investigator and author of this paper.
VITA

1991  B. Sc. in Electrical Engineering, Massachusetts Institute of Technology, Cambridge, MA.


2011  Ph. D. in Mathematics, University of California San Diego, La Jolla, CA.
ABSTRACT OF THE DISSERTATION

Implementing Measurements and Optimizing Queries for the Quantum Hidden Subgroup Problem

by

Asif Shakeel
Doctor of Philosophy in Mathematics
University of California San Diego, 2011

Professor David A. Meyer, Chair
Professor Nolan R. Wallach, Co-Chair

This dissertation concerns the Hidden Subgroup Problem (HSP) in quantum computation. We explore certain facets of the problem which, we expect, will lead towards a general framework for understanding such problems.

We first present an implementation of an optimal measurement, the Pretty Good Measurement (PGM), for the problem of the hidden subgroup problem over the dihedral group. This is a problem for which no efficient algorithm is known. This problem is relevant to the shortest vector in a lattice problem (SVP) in cryptography. We give a representation theoretic implementation of the PGM, achievable with only abelian transforms. The subset sum problem, an NP-complete problem, is needed in identification of certain subspaces. There are some novel ideas and techniques used in the implementation that make it realizable. This brings into focus how a measurement specified through a POVM (positive operator valued measure) is achievable through a basis change in a particular representation. This has connections to the HSP for other groups.

We also study the question of optimal query selection to maximize the probability of subgroup identification. This part of the research complements a well-researched topic of finding optimal measurements in the spirit of state discrimination as applied to the hidden subgroup problem. We find the optimal query, the
“character query”, over a class of queries that are an equal superposition over the group, for oracles that take values in a finite abelian group. This query outperforms the query used in the “standard method” of the HSP. This approach has connections to other domains of quantum computation.

We then extend the query selection idea to the case of multiple queries in the HSP and find examples in which this gives significant gains over the standard method. We consider the problems that the analysis of this more general problem entails, and outline a possible program to be followed. This is a part of continuing research.
Chapter 1

Introduction

1.1 Background

What makes quantum computation an interesting topic of study? To answer that question, one first needs to understand the problems of interest in classical computation (most of the material in this section can be read in [1-3]).

Classical computation is defined in terms of the Turing machine model. An input to the Turing machine can be considered to be a string of binary digits (bits), where \( n \) is the size of the input. In the Turing machine model the space and number of time steps available to execute an algorithm are unbounded. In practical computing applications, time and space resources are finite. This leads to the idea of computational complexity. The following complexity classes are basic and important. First is \( \text{P} \) which is the class of problems that can be solved in time \( \text{poly}(n) \). Second is \( \text{NP} \) which is informally the class of problems whose solutions can be checked in time \( \text{poly}(n) \) (for formal definitions, refer to [1]). It is not known, but strongly suspected that \( \text{P} \neq \text{NP} \). Another important class is \( \text{PSPACE} \) which consists of the problems that can be solved with \( \text{poly}(n) \) space resources in unbounded time. It follows that: \( \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} \).

An example of a problem which is not known and not expected to be in \( \text{P} \) (but is in \( \text{NP} \)) is the prime factorization of a number. How is this connected to the study of quantum computation? Before getting to that, let us examine the model of computation described by quantum computation.
Quantum computation is a model based on the axioms of quantum physics. The classical model of computation with information encoded by strings of binary digits (bits) is replaced by a model in which information is encoded by unit norm vectors (called pure states) in a Hilbert space $V$ over $\mathbb{C}$ (assume finite dimensional). If $v, x \in V$, we write the inner product $\langle v | x \rangle$. Following Dirac notation, “ket” $|v\rangle$ is the same as vector $v$ and “bra” $\langle v |$ is the linear functional that takes the value $\langle v | x \rangle$ on $x$. More generally a state is a Hermitian operator $\rho \in \text{End}(V)$ of unit trace, called the density operator or a mixed state. For a pure state $|v\rangle$ the density operator would be $\rho = |v\rangle \langle v |$. In contrast with the operations on bits through irreversible logic gates in classical computation, these states are only allowed to evolve by arbitrary unitary operations. A unitary operator $U$ transforms a state $\rho$ to $U \rho U^\dagger$.

Observations interact with the system through measurements, described by the POVM (positive operator valued measure). A POVM is a finite set of positive operators $\mathcal{E} := \{ E_k \}$. These satisfy: $\sum_k E_k = I$, where $I$ is the identity operator on $V$. If the system is in state $\rho$ prior to measurement, then as a result of the measurement, outcome $k$ is observed with probability $\text{tr}(E_k \rho)$, with the system in the post-measurement state:

$$\rho_k = \frac{\sqrt{E_k} \rho \sqrt{E_k^\dagger}}{\text{tr}(E_k \rho)}$$

In practical situations, a measurement is a choice of orthonormal basis. For a general measurement, there is no known procedure to implement it efficiently.

For the purposes of this thesis, we take all the vector spaces to be finite dimensional. One typically encounters mixed states if $V$ is a sub-system of a larger composite system given by a tensor product: $Y = V \otimes W$. Suppose the state of the system $Y$ is a pure state $|y\rangle \in Y$, then the state with respect to measurements confined to $V$ can be taken as the partial trace of the pure state $|y\rangle \langle y |$ over $W$: $\rho = \text{tr}_w (|y\rangle \langle y |)$, a mixed state. Partial trace operation is a linear map:

$$\text{tr}_w : \text{End}(V \otimes W) \rightarrow \text{End}(V)$$
which can be described using the inverse of the obvious isomorphism:

\[ \alpha : \text{End}(V) \otimes \text{End}(W) \cong \text{End}(V \otimes W) \]

\[ \alpha(f \otimes g)(v \otimes w) = f(v) \otimes g(w) \]

\[ \text{tr}_W : \text{End}(V) \otimes \text{End}(W) \to \text{End}(V) \]

\[ \sum_i R_i \otimes S_i \mapsto \sum_i \text{tr}(S_i)R_i \]

Let \( |y\rangle = \sum_i |v_i\rangle \otimes |w_i\rangle \) with \{\(|w_i\rangle\)\} orthonormal. Then:

\[ \text{tr}_W(|y\rangle \langle y|) = \sum_i |v_i\rangle \langle v_i| \]

A quantum algorithm consists of a sequence of unitary transformations and measurements, such that transformations in successive steps can be controlled by the result of processing of measurements in the previous step. A relevant complexity class for quantum computation is \( \text{BQP} \) consisting of problems that can be solved with a bounded probability of error on a quantum computer in \( \text{poly}(n) \) steps. It is also known that \( \text{P} \subseteq \text{BQP} \subseteq \text{PSPACE} \). It is not known if \( \text{P} \not\subseteq \text{BQP} \). If one can solve efficiently on a quantum computer a problem known not to be in \( \text{P} \), that would imply both the strict inclusion and \( \text{P} \neq \text{PSPACE} \). In general, there is a need to understand which problems are efficiently solvable using quantum computation.

Prime factorization has been shown by Shor [7] to be efficiently solvable on a quantum computer, and is the most significant indication yet of the power of quantum computation. It is based on well-known algorithm by Shor for the Quantum Fourier transform (QFT). Computation of discrete logarithm and algorithms for a host of other problems is also based on QFT.

Classical computational circuits, which are finite size implementations of Turing machines, are built from logic gates. Each logic gate is a function \( f : \mathbb{Z}_2^k \to \mathbb{Z}_2^l \). The basic building block of classical logic is the NAND gate, which implements a
function NAND : $\mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2$ given by:

$$\text{NAND} : (x_1, x_0) \mapsto (1 + x_1 \cdot x_0)$$

The NAND gate has the symbol:

![NAND gate](image)

Figure 1.1: NAND gate

Using the NAND gate, with the provision of some extra bits, an ability to copy bits, and ensuring that there are no loops, any logic gate and eventually any circuit can be built.

NAND is clearly irreversible. There is a reversible gate, the Toffoli gate, which can replace the NAND and hence is also universal for classical computation. $\text{Toffoli} : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^3$, is the map:

$$\text{Toffoli} : (x_2, x_1, x_0) \mapsto (x_2 + x_1 \cdot x_0, x_1, x_0)$$

By setting $x_2 = 1$, the restricted map ($\mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2$): $(x_1, x_0) \mapsto (1 + x_1 \cdot x_0)$ is the NAND gate.

The Toffoli gate has the symbol:

![Toffoli gate](image)

Figure 1.2: Toffoli gate

Turning to the quantum computation model, an operation is given by a unitary operator $U : \mathbb{C}^2 \rightarrow \mathbb{C}^2$. It can be shown (by construction) that an arbitrary
unitary operator can be implemented by two-qubit unitary operations, which in turn can be implemented by a Controlled-NOT (CNOT : \( \otimes^2 \mathbb{C}^2 \rightarrow \otimes^2 \mathbb{C}^2 \)) gate and one qubit operations. CNOT is given by the following action on the basis elements:

\[
\text{CNOT} : (x_1, x_0) \mapsto (x_1 + x_0, x_0)
\]

The CNOT gate has the symbol:

![CNOT gate diagram](image)

Figure 1.3: CNOT gate

Whether the implementation obtained by the above construction is efficient is another issue. Shor’s QFT algorithm is efficient by the clever reduction of the general Fourier transform on \( \otimes^n \mathbb{C}^2 \) to multiple uses of a set of operations consisting of a controlled phase changes, and the Hadamard transform (Fourier transform on \( \mathbb{Z}_2 \)). The Hadamard transform \( H \) is described by its action on the computational basis:

\[
H : \begin{cases} 
|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =: |+\rangle \\
|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |\rangle
\end{cases}
\]

As part of Shor’s algorithm, the QFT is computed and the result of the measurement in the computational basis (\( \{|k\rangle : k \in \mathbb{Z}_{2^n} \} \)) is used to compute the period of a function. This is a characteristic of many quantum algorithms that partial measurements (incomplete Von-Neumann measurement), classical operations, and unitary operations are performed at intermediate stages.

Reductions as in QFT are in general not possible, so any quantum algorithm (defined above as a sequence of unitary operations, measurements and classical processing) must be analyzed carefully to determine the size of the circuit and number of steps needed to execute it.

At some point in every quantum algorithm, a measurement is made prior to
final classical processing of the measurement data. This makes the choice of measurement critical to the success of an algorithm. The subject of measurements is a well-researched branch of quantum algorithms. It is often hard to find an appropriate measurement that would yield the most relevant information. Even if a useful measurement can be determined, it is not usually obvious how to choose an appropriate set of basis for the measurement, or how to implement it efficiently using known or efficiently implementable quantum operations.

Since every quantum algorithm evolves a state in some Hilbert space, the choice of initial state of the system (the query) has implications as important as the measurement. In fact, the two are related closely since a measurement can in some sense only be as good as the information contained in the final state of the system prior to the measurement. As the final state is naturally dependent on the initial state, query selection is of much interest.

With this abundance of competing notions, how does one algorithm compare with another? Computational complexity is an accepted comparison for those algorithms that have an implementation. When no implementable algorithm is known, can algorithms still be compared? Then the next consideration is if the number of oracle calls, or queries, is polynomially bounded in the size of the input. This is the idea of query complexity. Another comparison when the complexity classes can not be compared, or when comparing algorithms in the same complexity class, is that of the probabilities of successfully yielding the solution.

That leads to the question of optimality. From the computational complexity point of view, an optimal algorithm is one that solves the problem with the minimum of computational resources. When using the probability of successfully finding a solution as a criterion of comparison, an optimal algorithm can also be defined as one yielding the highest probability. One notes that computationally efficient algorithms may not be those that yield maximum probability of success and vice versa.
1.2 The Hidden Subgroup Problem (HSP)

Some of the most interesting problems in this field of research can be formulated as search problems. Continuing with our example of prime factorization, one of the first known practical applications evolved out of the reduction by Shor [7] of prime factorization of a composite $N \in \mathbb{Z}$ to period search of a function. The specific function in this case is known and it is easy to calculate each value classically, but the determination of period by sampling values involves $O(N)$ evaluations of the function. This is an instance of the Hidden Subgroup Problem (HSP) in which the period of the function “hides” a subgroup of $\mathbb{Z}_N$, i.e., the function is constant and distinct on cosets of some subgroup of $\mathbb{Z}_N$. The quantum algorithm begins by collapsing the function to a coset of the “hidden” subgroup. Quantum measurements based on the use of Shor’s highly efficient Quantum Fourier Transform (QFT) then find the subgroup, hence the period, in $\text{poly}(\log(N))$ computations.

More generally, the function is provided by an oracle that evaluates it as a unitary transformation on a superposition of the elements of some group $G$, presented to the oracle via “queries”. The concept is generalized via the general HSP [15] which can be stated as:

**Hidden Subgroup Problem (HSP)** Let $G$ be a group, $X$ a finite set, and $f : G \to X$ a function. There exists a subgroup $H \leq G$ such that $f$ is constant and distinct on the cosets (assume left cosets) of $H$. That is, the function has the property:

$$f(gh) = f(g) \quad \forall h \in H, \ g \in G$$

and $f(g) = f(g') \iff g' \in gH$. $f$ is accessed via queries to an oracle. Using information gained from evaluations of $f$ via its oracle, determine a generating set for $H$.

In this particular case, one thinks of the Hilbert space $Y = \mathbb{C}[G] \otimes \mathbb{C}[X]$ as the system on which the oracle and measurement act. A query is a unit norm state in $Y$ to be presented to the oracle. An oracle implementing a function $f$ is described
by the unitary operator $O_f$ which acts on a basis state $|g\rangle \otimes |x\rangle \in Y$ by:

$$O_f : |g\rangle \otimes |x\rangle \mapsto |g\rangle \otimes |x + f(g)\rangle$$

under the assumption that $X$ is an abelian group. Although this assumption is not required by the general HSP, it is used in some existing algorithms and interesting cases in the literature (e.g., Regev’s reduction of the Unique-SVP [5]). $\mathbb{C}[G]$ is called the query register, and $\mathbb{C}[X]$ is called the response register. Search for the subgroup generators has to be done by an efficient algorithm which can use unitary transformations, quantum measurements, and classical processing. Measurements and queries are central to the HSP.

An algorithm for a given HSP is considered successful if it can compute the generators of the hidden subgroup with a probability greater than some constant. Then a polynomial number of trials can make the algorithm succeed with arbitrarily high probability. An algorithm is said to be query-efficient if the number of queries to the oracle and measurements it requires to solve the HSP is upper bounded by a fixed polynomial in the size of the group $\log(|G|)$, i.e., it is $\text{poly}(\log(|G|))$ in the number of queries. It is computationally efficient (or efficient) if the resources required to carry out the computations needed to implement the unitary operations and measurements are $\text{poly}(\log(|G|))$.

HSP over an abelian group is solved using the QFT (the version called the Abelian Stabilizer Problem was defined and solved by by Kitaev [4]). The generalization above moves the HSP beyond the abelian group $\mathbb{Z}_N$ of prime factorization or the discrete logarithm problem [7]. Now several groups of interest show up as underlying groups for classical problems from known areas of investigation. The search for the unique shortest vector in a lattice problem (Unique-SVP) in cryptography, and the graph isomorphism problem are two of them. The graph isomorphism problem requires an algorithm for the HSP over the symmetric group, and the Unique-SVP that for the dihedral group. The reduction of the graph isomorphism to the HSP over the symmetric group was due to Ettinger and Høyer [8], and that of the Unique-SVP to the HSP over the dihedral group due to Regev [5].

Several families of groups have been investigated, and efficient HSP algorithms
found for many of them. A comprehensive recap of the results can be found in [9, 10]. There are still a number of groups that have no known efficient algorithms. Both the symmetric group and the dihedral group cases belong to this category.

The earliest HSP, as stated, was over finite abelian groups, and efficient algorithm is known for this case [10]. With the introduction of non-abelian groups, more complex algorithms are required. One of the first results is that a polynomial number of queries is sufficient to solve HSP over a finite group [13]. Next is the computational efficiency, but to the author’s knowledge, no general bounds for this have been established.

Quantum information processing is the other ingredient of any algorithm. This includes any unitary operation on the state of the system. For abelian groups, the main tool is the abelian QFT. The counterpart for non-abelian groups is the non-abelian Fourier transform over the group. Significant progress in HSP algorithms comes from the use of representation theory [16, 20–22, 25]. For some interesting families of groups, efficient Fourier transforms have been found [17]. In a number of cases, implementation of some measurement in the Fourier basis then solves the HSP. In general, this is a hard problem. Even when all the representations of a group are known, the Fourier transform may not be efficiently implementable or there may not be a way to exploit it. For an efficient algorithm, moreover, measurements also need to be implemented efficiently.

1.3 Basic representation theory of finite groups

We will also need some basic results from the representation theory of finite groups, and this material is condensed from [26]. We recall the definitions for our purposes.
1.3.1 Definitions

A representation of \( G \) is a pair \((\rho, V)\), where \( V \) is a complex vector space, and \( \rho : G \to \text{GL}(V) \) is a group homomorphism.

The space of complex functions \( \mathbb{C}[G] \) on \( G \), called the group algebra of \( G \), is an associative algebra under the convolution \((\ast)\) multiplication. Given \( \phi, \vartheta \in \mathbb{C}[G] \), their product \( \phi \ast \vartheta \) is defined to be:

\[
(\phi \ast \vartheta)(g) = \sum_{h \in G} \phi(h)\vartheta(h^{-1}g)
\]

Every representation \((\rho, V)\) of \( G \) extends uniquely by linearity to a representation \( \rho \) of \( \mathbb{C}[G] \) (using the same symbol), i.e., \( \rho : \mathbb{C}[G] \to \text{End}(V) \) is an algebra homomorphism.

If \((\rho, V)\) and \((\tau, W)\) are representations of \( G \), define \( \text{Hom}_G(V, W) \) as follows:

\[
\text{Hom}_G(V, W) = \{ T \in \text{Hom}(V, W) : \tau(g)T = T\rho(g) \}
\]

Two representations \( \rho \) and \( \tau \) are equivalent if there exists an invertible map in \( \text{Hom}_G(V, W) \). In this case we write \( \rho \cong \tau \).

Let \((\rho, V)\) be a representation of \( G \). A subspace \( W \subset V \) is \( G \)-invariant if \( \rho(g)w \in W \) for all \( g \in G \) and \( w \in W \). A representation \((\rho, V)\) is reducible if there is a \( G \)-invariant subspace \( W \subset V \) such that \( W \neq \{0\} \) and \( W \neq V \). A representation that is not reducible is called irreducible.

Given a representation \((\rho, V)\), the dual representation \((\rho^*, V^*)\) is given by:

\[
\langle \rho^*(z)v^*, v \rangle = \langle v^*, \rho(z^{-1})v \rangle
\]

for \( z \in G, v \in V \), and \( v^* \in V^* \).

Let \((\rho, V)\) and \((\sigma, W)\) be finite-dimensional representations of \( G \). There is a representation called the tensor product \((\rho \otimes \sigma, V \otimes W)\) of the two representations, defined by:

\[
(\rho \otimes \sigma)(g) = \rho(g) \otimes \sigma(g)
\]
There is also a representation $\pi$ of $G$ on $\text{Hom}(V, W) \cong W \otimes V^*$, given by:

$$\pi := \sigma \otimes \rho^*$$

Let $G = H \times K$, be the direct product of two groups. Let $(\rho, V)$ and $(\tau, W)$ be finite-dimensional representations of $H$ and $K$ respectively. Then the outer tensor product $(\rho \hat{\otimes} \tau, V \otimes W)$ representation of $G$ is defined by:

$$(\rho \hat{\otimes} \tau)(h, k) = \rho(h) \otimes \tau(k) \quad \text{for } h \in H, k \in K$$

For the rest of the discussion, let $\hat{G}$ be the equivalence classes of irreducible representations of $G$, and fix a model $(\pi^\lambda, V^\lambda)$ in the class $\lambda$ for each $\lambda \in \hat{G}$.

### 1.3.2 The group algebra $\mathbb{C}[G]$}

One of the fundamental results about irreducible representations of $G$ is Schur’s Lemma:

**Lemma.** Let $(\rho, V)$ and $(\tau, W)$ be irreducible representations of a group $G$. Then

$$\dim \text{Hom}_G(V, W) = \begin{cases} 1 & \text{if } (\rho, V) \cong (\tau, W) \\ 0 & \text{otherwise} \end{cases}$$

We denote by $L$ and $R$ the left and right translation representations of $G$ on $\mathbb{C}[G]$.

$$L(z)\phi(g) := \phi(z^{-1}g)$$

$$R(z)\phi(g) := \phi(gz) \quad (1.1)$$

We extend the left and right translation representations of $G$ on $\mathbb{C}[G]$ by linearity to get the left and right regular representations of $\mathbb{C}[G]$ on itself, also denoted by $L$ and $R$:

$$L, R : \mathbb{C}[G] \to \text{End}(\mathbb{C}[G])$$

The group $G \times G$ acts on $\mathbb{C}[G]$ by left and right translations. Denote this
representation by $\tau$:

$$\tau(z, w)\phi(g) = \phi(z^{-1}gw) \quad \text{for } z, g, w \in G$$

For $\lambda \in \hat{G}$, define the map:

$$\varphi_{\lambda}(v^* \otimes v)(g) = \langle v^*, \pi^\lambda(g)v \rangle$$

for $g \in G, v^* \in V^\lambda$ and $v \in V^\lambda$. Extend $\varphi_{\lambda}$ to a linear map from $V^\lambda \otimes V^\lambda$ to $\mathbb{C}[G]$. Then:

1. Range($\varphi_{\lambda}$) provides an irreducible $G \times G$ representation (restriction of $\tau$ to Range($\varphi_{\lambda}$)) isomorphic to the outer product representation $(\pi^\lambda \otimes \pi^\lambda, V^\lambda \otimes V^\lambda)$ given by:

$$\pi^\lambda \otimes \pi^\lambda(z, w) = \pi^\lambda(z) \otimes \pi^\lambda(w)$$

2. The space $\mathbb{C}[G]$ decomposes as:

$$\mathbb{C}[G] = \bigoplus_{\lambda \in \hat{G}} \varphi_{\lambda}(V^\lambda \otimes V^\lambda)$$

(1.3)

With the decomposition in (1.3), the left translation is isomorphic to:

$$L(z) \cong \bigoplus_{\lambda \in \hat{G}} \pi^\lambda(z) \otimes I_{V^\lambda}$$

and the right translation is isomorphic to:

$$R(z) \cong \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda} \otimes \pi^\lambda(z)$$

where $I_{V^\lambda}$ and $I_{V^\lambda^*}$ are identity operators on the spaces $V^\lambda$ and $V^\lambda^*$ respectively. Under the isomorphism $V^\lambda \otimes V^\lambda \cong \text{End}(V^\lambda)$ sending $v^* \otimes v$ to the operator $u \mapsto \langle v^*, u \rangle v$, the isomorphism $\varphi_{\lambda}$ in (1.2) becomes $\varphi_{\lambda}(T)(g) = \text{tr}(\pi^\lambda(g)T)$ for $T \in \text{End}(V^\lambda)$. $(z, w) \in G \times G$ acts by $T \mapsto \pi^\lambda(w)T\pi^\lambda(z^{-1})$ on the $\lambda$ summand.
The decomposition of $\mathbb{C}[G]$ in (1.3) becomes:

$$\mathbb{C}[G] \cong \bigoplus_{\lambda \in \hat{G}} \text{End}(V^\lambda)$$

Since $\dim \mathbb{C}[G] = |G|$ and $\dim \text{End}(V^\lambda) = d_\lambda$, the above isomorphism implies:

$$|G| = \sum_{\lambda \in \hat{G}} d_\lambda^2$$

### 1.3.3 The Fourier transform

Every irreducible representation of a finite group $G$ is finite dimensional, and has a positive definite $G$-invariant Hermitian inner product (average any inner product over $G$). Then every model $(\pi_\lambda, V^\lambda)$ for $\lambda \in \hat{G}$ can be taken to be unitary.

The space $V^{\lambda^*}$ can be taken to be $V^\lambda$ with:

$$\pi^{\lambda^*}(g) = \bar{\pi^\lambda(g)}$$

From the previous section, under $G \times G$ action:

$$\mathbb{C}[G] \cong \bigoplus_{\lambda \in \hat{G}} \text{End}(V^\lambda)$$

Given $f \in \mathbb{C}[G]$ and $\lambda \in \hat{G}$, define an operator $\mathcal{F} f(\lambda)$ on $V^\lambda$:

$$\mathcal{F} f(\lambda) := \sum_{x \in G} f(x) \pi^\lambda(x)$$

The Fourier transform $\mathcal{F}$ is the map:

$$\mathcal{F} : \mathbb{C}[G] \rightarrow \bigoplus_{\lambda \in \hat{G}} \text{End}(V^\lambda)$$

$$f \mapsto \{ \mathcal{F} f(\lambda) \}_{\lambda \in \hat{G}}$$

(1.4)
The Fourier transform is an algebra isomorphism. It satisfies:

\[ \mathcal{F}(L(g)f)(\lambda) = \pi^\lambda(g) \mathcal{F}f(\lambda) \]
\[ \mathcal{F}(R(g)f)(\lambda) = \mathcal{F}f(\lambda) \pi^{\lambda}(g^{-1}) \]

The inverse of Fourier transform is given by the Fourier Inversion Formula:

\[ \mathcal{F}^{-1} : \bigoplus_{\lambda \in \hat{G}} \text{End}(V^\lambda) \to \mathbb{C}[G] \]
\[ F = \{ F(\lambda) \}_{\lambda \in \hat{G}} \mapsto f = \frac{1}{|G|} \sum_{\lambda \in \hat{G}} d_\lambda \text{tr}(\pi^\lambda(g)F(\lambda)^t) \] (1.5)

\( \mathbb{C}[G] \) has an inner product:

\[ \langle \phi | \vartheta \rangle = \sum_{g \in G} \overline{\phi(g)} \vartheta(g) \]

where \( \phi, \vartheta \in \mathbb{C}[G] \).

One obtains the Plancherel Formula. Let \( \varphi, \psi \in \mathbb{C}[G] \). Then:

\[ \langle \varphi | \psi \rangle = \sum_{g \in G} \varphi(g) \overline{\psi(g)} = \frac{1}{|G|} \sum_{\lambda \in \hat{G}} d_\lambda \text{tr}(\mathcal{F}\varphi(\lambda)\mathcal{F}\psi(\lambda)^*) \]

For \( T \in \text{End}(V^\lambda) \), \( T^* \) denotes the adjoint operator of \( T \) relative to the \( G \)-invariant inner product on \( V^\lambda \).

\[ \langle Tu, v \rangle = \langle u, T^* v \rangle \]

1.3.4 Characters and projections

The character of a representation \((\rho, V)\) of a group \(G\) is a function:

\[ \chi_\rho : G \to \mathbb{C}^* \]
\[ g \mapsto \text{tr}(\rho(g)) \]
Let $\lambda, \mu \in \hat{G}$, then it follows that:

$$\mathcal{F} \chi_{\lambda}(\mu) = \begin{cases} 
\frac{|G|}{a_{\lambda}} I_{V^\lambda} & \text{if } \mu = \lambda \\
0 & \text{otherwise}
\end{cases}$$

Then using the Plancherel formula we see:

$$\langle \chi_{\lambda} | \chi_{\mu} \rangle = \begin{cases} 
1 & \text{if } \mu = \lambda \\
0 & \text{otherwise}
\end{cases}$$

Suppose $(\rho, V)$ is any finite-dimensional representation of $G$. It is can be shown that $V$ decomposes as follows:

$$V \cong \bigoplus_{\lambda \in \hat{G}} \text{Hom}_G(V^\lambda, V) \otimes V^\lambda$$

Set:

$$m_V(\lambda) = \dim \text{Hom}_G(V^\lambda, V) \quad \text{for } \lambda \in \mathbb{C}[G]$$

$\text{Hom}_G(V^\lambda, V) \otimes V^\lambda$ is called the $\lambda$-isotypic subspace of $V$, $\text{Hom}_G(V^\lambda, V)$ the multiplicity space of $\lambda$, and $m_V(\lambda)$ the multiplicity of $\lambda$ in $V$. $g \in G$ acts by:

$$\rho(g) \cong \bigoplus_{\lambda \in \hat{G}} I_{\text{Hom}_G(V^\lambda, V)} \otimes \pi^\lambda(g)$$

Here $I_{\text{Hom}_G(V^\lambda, V)}$ is the identity operator on $\text{Hom}_G(V^\lambda, V)$. This says:

$$\chi_{\rho} = \sum_{\lambda \in \hat{G}} m_{\rho}(\lambda) \chi_{\lambda}$$

An important result is that $m_{\rho}(\lambda) = \langle \chi_{\rho} | \chi_{\lambda} \rangle$ and:

$$\langle \chi_{\rho} | \chi_{\rho} \rangle = \sum_{\lambda \in \hat{G}} m_{\rho}(\lambda)^2$$
In particular $\rho$ is irreducible if and only if $\langle \chi_\rho | \chi_\rho \rangle = 1$. The operator:

$$P_\lambda = \frac{d_\lambda}{|G|} \sum_{g \in G} \chi_\lambda(g) \rho(g)$$

is the projection onto the $\lambda$-isotypic subspace of $V$.

### 1.3.5 Notation and frequently used results

1. To rephrase the above in terms of the “ket” notation, we introduce the computational basis of $\mathbb{C}[G]$ consisting of the $\delta$ functions:

$$\delta_g(g') = \begin{cases} 1, & g' = g \\ 0, & \text{otherwise} \end{cases}$$

We also write $|g\rangle := \delta_g$. Then an element $|\phi\rangle \in \mathbb{C}[G]$ has a unique expression as a sum $|\phi\rangle = \sum_{g \in G} \phi(g) |g\rangle$.

Then the left and right translation representations ($L$ and $R$) of $G$ on $\mathbb{C}[G]$ can be described in the “ket” notation. On the element:

$$|\phi\rangle = \sum_{g \in G} \phi(g) |g\rangle \in \mathbb{C}[G],$$

$z \in G$ acts by:

$$L(z) |\phi\rangle = \sum_{g \in G} \phi(g) |zg\rangle = \sum_{g \in G} \phi(z^{-1}g) |g\rangle$$

$$R(z) |\phi\rangle = \sum_{g \in G} \phi(g) |gz^{-1}\rangle = \sum_{g \in G} \phi(gz) |g\rangle$$

This connects the translation representation on functions to that on the “ket” notation of vector spaces.

2. Let $G$ be a group. Suppose $T \in \text{End}(\mathbb{C}[G])$ commutes with left translations by $G$. Then there is a function $\phi \in \mathbb{C}[G]$ such that $T(\varphi) = \varphi * \phi$ (convolution product) for all $\varphi \in \mathbb{C}[G]$. 
Consider the action of $T$ on $\delta_1$:

$$T(\varphi * \psi) = \varphi * T(\psi) \quad \forall \varphi, \psi \in \mathbb{C}[G]$$

$$\implies T(\varphi) = \varphi * T(\delta_1)$$

3. The notation for tensor products used in quantum computation is as follows. An element $|u\rangle \otimes |v\rangle$ of a tensor product of vector spaces $U, V$ is denoted:

$$|u\rangle|v\rangle := |u\rangle \otimes |v\rangle \in U \otimes V$$

We utilize this notation when it is unambiguous to do so.

## 1.4 Summary of approaches and techniques

We briefly examine some of the approaches to select the query and measurements as found in the literature.

### 1.4.1 Weak and strong Fourier sampling

These particular kinds of measurements apply mainly to the standard method and are defined in terms of representations.

(i) **Weak Fourier sampling:** This measurement distinguishes among the states by their projections on the isotypic components. Only the irreducible representation index is used in the classical processing of the measurement.

One such example is the case of the HSP over the set of normal subgroups of a group [6]. Weak Fourier sampling followed by classical processing of the irreducible representation label yields the subgroup with high probability.

(ii) **Strong Fourier sampling:** This measurement distinguishes among the states by choosing some orthogonal basis for each isotypic component, and projecting on the individual elements of the bases enumerated over all the representations. Hence, not only the representations indices are distinguished,
but the elements of the basis within the isotypic components as well. These are then processed in determining the hidden subgroup.

One such example is the Heisenberg group $[11, 12]$ in which the invariants of the subgroups within the sub-representations are distinguished to identify the subgroup.

### 1.4.2 Subgroup reduction

For certain groups, it is possible to reduce the problem from its most general form to one in which only a subset of all the subgroups are to be searched. Reasons for such reductions vary, and can be dependent on the structure of the group as well as having access to efficient algorithms for certain class of subgroups. Quotient by or inclusion in (or a chain of inclusions) such subgroups can greatly simplify the problem. Among examples of groups where such reductions are taken advantage of are the dihedral group $[14]$ and the Heisenberg group $[11]$.

For the dihedral group, Ettinger and Høyer $[14]$ reduce the problem of identifying an arbitrary subgroup to the identification of order two subgroups generated by a single reflection, and the trivial subgroup consisting of the identity.


### 1.4.3 Single-query vs multi-query

The algorithms are also widely obtained and can vary from single-query algorithms to multi-query ones. Multi-query algorithms are differentiated based on the mode in which the oracle responses to queries are utilized. In a purely sequential queries strategy, the post-query state can be modified and presented back to the oracle in succession. In parallel queries strategy, the state is contained in a tensor product of Hilbert spaces, each identical to that for the single-query. Several identical oracles respond to different tensor factors of the state.

Parallel queries have been used in several algorithms. Sometimes this is used with a single measurement as in $[20, 21]$. On other occasions, the processing of
queries is highly dependent on the structure of the group and its subgroups, and some methods (like sieving used by Kuperberg [27] and Regev [28]) are sophisticated in their use of combination of statistical ideas and the use of a parallel queries, transforms and intermediate measurements to develop and retain states with improved information about the hidden subgroup.

1.4.4 The standard method in HSP

The context is as follows. We have a set $\mathcal{S} = \{H_l\}_{l \in \mathcal{L}}$ of subgroups of a finite group $G$, indexed by a finite set $\mathcal{L}$.

The measurement $\mathcal{E} = \{E_k\}_{k \in \mathcal{X}}$ is as described in section 1.1, i.e., a set of positive operators on the query register $\mathbb{C}[G]$, satisfying $\sum_k E_k = I$, where $I$ is the identity operator. The measurement operator $E_k$ corresponds to the outcome $k$, associated to the state $H_k$.

A single-query HSP algorithm (generalizable to a parallel multi-query algorithm) to identify a subgroup from the set $\mathcal{S}$ comprises the following steps:

(i) Prepare the query $|\Psi\rangle \in \mathbb{C}[G] \otimes \mathbb{C}[X]$.

(ii) Evaluate the oracle on $|\Psi\rangle$.

(iii) Measure the query register $\mathbb{C}[G]$ using a measurement $\mathcal{E} = \{E_k\}$. Observe the outcome $k$ and do classical processing of the outcome to decide upon some $H_l$ as the hidden subgroup.

The “standard method” [16] is so called because it starts in (i) with an equal superposition query with $|0\rangle$ in the response register: $|\Psi\rangle = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |0\rangle$. We call this the standard query.

As a remark, usually in the literature an additional step is inserted between steps (ii) and (iii), after the oracle evaluation and before the query register $\mathbb{C}[G]$ measurement. In this step, the response register $\mathbb{C}[X]$ is measured. This is not strictly necessary since the result of this measurement is not used in deciding the hidden subgroup. That decision is based on the measurement of the query register assisted with classical processing, and the measurement probabilities are
not affected by the optional measurement of the response register, as shown in Nielsen and Chuang [1].

1.4.5 State discrimination

State discrimination dates back to the 1970’s when it was developed in the context of quantum statistical decision theory by Holevo [18]. Yuen, Kennedy and Lax [19] developed a very important and useful set of results to include checkable conditions for optimal measurements.

State discrimination is stated as an optimization problem. One assumes that the system is in one of a set of possible states described by density operators \( \{\rho_k\}_{k \in \mathcal{K}} \) on some finite dimensional Hilbert space \( V \). These states are indexed by a finite set \( \mathcal{K} \), and distributed according to a probability function \( \{p_k\}_{k \in \mathcal{K}} \) such that \( p_k \) is the prior probability of occurrence of \( \rho_k \). The problem is to choose which of the states is the most likely candidate, based on the result of a measurement. As described in the background section, a measurement on \( V \) is described by a set of operators (POVM) \( \mathcal{E} := \{E_k\}_{k \in \mathcal{K}} \). These satisfy: \( E_k \geq 0 \) and \( \sum_{k \in \mathcal{K}} E_k = I \), where \( I \) is the identity operator. The measurement operator \( E_k \) corresponds to the outcome \( k \) (an observed quantity), such that the decision when \( k \) is observed is that the system is in the state \( \rho_k \). Then, given that the state is \( \rho_k \), the probability of correct decision is \( \text{tr} (E_k \rho_k) \). Considering the prior probability of occurrence of the states, the probability of successful state discrimination using a measurement \( \mathcal{E} := \{E_k\}_{k \in \mathcal{K}} \) is:

\[
S(\mathcal{E}) := \sum_{k \in \mathcal{K}} p_k \text{ tr} (E_k \rho_k)
\]  

A measurement is optimal if it maximizes \( S(\mathcal{E}) \) over the set of all measurements.

States to be discriminated in the HSP are mixed states of the system. Each state results from an oracle response to a query under the assumption that the oracle hides a particular subgroup. Therefore, there are at least as many states as the possible hidden subgroups. Optimality of measurements can be confirmed by verifying simple checkable criteria [18, 19]. This technique has been shown to be very useful [20–22] in works investigating optimal measurements.
A measurement \( \{E_k\}_{k \in \mathcal{K}} \) is optimal, i.e., maximizes \( S(\mathcal{E}) \) if and only if for all \( k \in \mathcal{K} \):

\[
\left( \sum_j p_j \rho_j E_j - p_k \rho_k \right) E_k = 0
\]

\[
\sum_j p_j \rho_j E_j = \sum_j p_j E_j \rho_j
\]

\[
\sum_j p_j \rho_j E_j \geq p_k \rho_k
\]
Chapter 2

The dihedral group HSP: an implementation of the Pretty Good Measurement (PGM)

As an outstanding problem, algorithm for the HSP over the dihedral group occupies a central position. Although it is an unsolved problem, there are interesting ideas that have been used in attempts to solve this problem. Bacon, Van Dam and Childs show that a kind of measurement, the Pretty Good Measurement (PGM) is optimal for the HSP over the dihedral group in the context of the standard method. Assuming the group is of cardinality $2^N$, their work shows that using $k = O(\log(N))$ parallel queries, this HSP can be solved. They show the connection to an underlying problem, the subset sum problem, an NP-complete problem. They conclude that an efficient “quantum sampling” of the solutions of the subset sum would lead to an efficient PGM implementation. The work of Moore and Russell provides a representation theoretic proof of the PGM optimality for HSP over conjugate subgroups of a group. The main result of this chapter is an explicit representation theoretic implementation of multi-query PGM for dihedral group. Some of the work draws upon the work of Moore and Russell. Using a natural choice of basis for the left translation representation of the group, making observations about the subset sum as it appears in this implementation, and obtaining rank 2 POVM implementing the Naimark extension, an algorithm is presented
that uses simple abelian transforms. The subset sum problem is needed in the identification, within the sub-representations, of certain subspaces (as in the work of Bacon et al.) essential to the algorithm.

2.1 Introduction

A number of results concerning the Hidden Subgroup Problem (HSP) of the dihedral group (let the cardinality of the group be $2N$) have been published. Among known algorithms, Kuperberg [27] provided an algorithm with subexponential (in $\log(N)$) query, time, and space complexity. Regev [28] further reduced the space complexity to be $\text{poly}(\log(N))$, with the query and time complexity still subexponential.

Other algorithms which have been studied require solutions to the subset sum problem, an NP-complete problem. These have been quantified by query complexity and their computational complexity depends on whether certain average case solutions to the subset sum problem can be found. The subset sum problem is: given an element $\vec{\mu} \in \mathbb{Z}_N^k$ and $z \in \mathbb{Z}_N$, is there a set $\vec{b} \in \mathbb{Z}_2^k$ (solution) such that $\vec{b} \cdot \vec{\mu} = \sum_{i=1}^k b_i \mu_i = z \mod N$. A pair $(\vec{\mu}, z)$ for which such a solution $\vec{b}$ exists is a legal instance of the subset sum.

Regev [5] shows that for $k > \log(N) + 4$, if one can efficiently find one solution to $1/\text{poly}(\log(N))$ of the legal instances, then there is an efficient algorithm for the HSP over the dihedral group of cardinality $2N$.

A particular measurement called the Pretty Good Measurement (PGM) has been studied by several authors. It has been shown to solve the dihedral HSP problem optimally, in the sense of maximizing the probability of successful subgroup identification, in the context of the ‘standard HSP algorithm’. The work of Bacon et al. [21] was the first to show the optimality, and show that $k \geq \log(N) + 4$ parallel queries suffice to successfully solve the HSP for the dihedral group of cardinality $2N$. For a legal instance $(\vec{\mu}, z)$, they define the set of solutions:

$$C_{\vec{\mu} z} := \{ \vec{b} \in \mathbb{Z}_N^k \mid \vec{b} \cdot \vec{\mu} = z \mod N \}$$
In terms of its cardinality \( \eta_z^{\bar{\mu}} := |C_z^{\bar{\mu}}| \), the probability of success is:

\[
\frac{1}{2^k \sqrt{2^{k+1}}} \sum_{\bar{\mu} \in \mathbb{Z}_N^k} \left( \sum_{z \in \mathbb{Z}_N} \sqrt{\eta_z^{\bar{\mu}}} \right)^2
\]

In studying possible implementation, they find that an equal superposition state of solutions from the set \( C_z^{\bar{\mu}} \) for every legal instance \((\bar{\mu}, z)\), a “quantum sample” of solutions, would be needed to implement the PGM exactly. That implies that the complexity and success probability of a PGM based HSP algorithm can be quantified up to those of the subset sum.

These results are captured by the definition of the density \( \nu = k/\log(N) \). Then both Regev [5] and Bacon et al. [21] are concerned with the \( \nu \sim 1 \) regime. Also, as demonstrated in [21], the PGM has a sharp threshold in probability of success at \( \nu \sim 1 \), going from exponentially small in \( \log(N) \) to above a constant. They explain that these algorithms do not require a solution to the most general subset sum problem. In Regev, a random solution to a fraction of legal instances is needed, an average-case subset sum scenario. In Bacon et al., a “quantum sample” is needed, which can be considered a quantum version of the average-case of the classical version.

We translate the PGM to an algorithm via the left translation action of the dihedral group, results of Moore and Russell [20] providing part of the necessary framework. In this vein, we describe the representation of the dihedral group as relevant to the problem and computations on the group algebra. We choose a natural basis for the left translation representation of the group, which make the basis change to the representation basis a tensor of Hadamard transform and the Fourier transform over \( \mathbb{Z}_N \). The structure of the problem as it appears in the this basis determines some choices. We see that it is more useful to compute the subset sum (mod 2N) to help diagonalize the measurements. Though it is known that measurements that are not projections on an orthonormal basis of a Hilbert space can be made into such orthogonal projective measurements by embedding the space in a higher dimensional space (Naimark extension theorem), it is not always possible to find an embedding by simple transforms. We construct such
an embedding, and show the final result of the measurement in the computational basis. The measurement is a set of rank 2 projections on orthogonal subspaces. It is attainable as an inverse Fourier transform over \( \mathbb{Z}_{2N} \), followed by a union of two measurements, each acting on a partition of computational basis of \( \mathbb{C}[\mathbb{Z}_{2N}] \). This requires some ideas and observations that lead to making these measurement realizable. We show where and how the solution of the subset sum would be used to rotate the subspaces and get the equal superposition states over the subset sum solutions, the “quantum sampling”. This, in a sense, isolates the subset sum problem and can help understand the impact of inexact subset sum solution.

This chapter is organized as follows. In Section 2 we restate the standard method in HSP. In Section 3 we use the representation to examine the PGM for a single query and specialize it to the dihedral group. In Section 4 we generalize the problem to multiple queries, recall the multi-query framework for this problem, and look at the PGM in terms of the representation. In sections 5, 6, 7 we present the algorithms for single and multiple queries. In section 8 we study the probability of success and complexity. Section 9 is the conclusion and suggests future direction.

### 2.2 The standard method

General Dihedral HSP consists of identifying an arbitrary subgroup of dihedral group given a function constant on cosets of an unknown hidden subgroup of \( G \).

At the outset, we note that instead of usual statement in terms of left cosets of the hidden subgroup, we choose to work with right cosets. The rationale for doing so will become clear in the course of our work.

We restate the general HSP [15]:

**Hidden Subgroup Problem (HSP)** Let \( G \) be a group, \( X \) a finite set, and \( f : G \rightarrow X \) a function. There exists a subgroup \( H \leq G \) such that \( f \) is constant and distinct on the cosets (assume left cosets) of \( H \). That is, the function has the property:

\[
f(gh) = f(g) \quad \forall h \in H, \ g \in G
\]

and \( f(g) = f(g') \iff g' \in gH \). \( f \) is accessed via queries to an oracle. Using
information gained from evaluations of \( f \) via its oracle, determine a generating set for \( H \).

We define the set of possible hidden subgroups \( \mathcal{S} = \{ H_l \}_{l \in \mathcal{L}} \) of \( G \) indexed by a finite set \( \mathcal{L} \) of cardinality \( L := |\mathcal{L}| \). For a subgroup \( H_l \in \mathcal{S} \), we denote its index by \( N_l := [G : H_l] \). The probability that the oracle function hides any particular subgroup \( H_l \in \mathcal{S} \) is \( 1/L \).

The standard method of HSP is as follows. We start with the Hilbert space (applicable to single-query algorithm, and generalizable to multiple queries in parallel) which is a tensor product of \( \mathbb{C}[G] \) (the query register) and \( \mathbb{C}[X] \) (the response register):

\[
\mathcal{H} = \mathbb{C}[G] \otimes \mathbb{C}[X]
\]

We assume that \( X \) is abelian, an assumption in much of the HSP literature.

We introduce the computational basis of \( \mathbb{C}[G] \) consisting of the \( \delta \) functions:

\[
\delta_g(g') = \begin{cases} 
1, & g' = g \\
0, & \text{otherwise}
\end{cases}
\]

We also write \( |g\rangle := \delta_g \). Then an element \( |\phi\rangle \in \mathbb{C}[G] \) has a unique expression as a sum \( |\phi\rangle = \sum_{g \in G} \phi(g)|g\rangle \).

\( \mathbb{C}[G] \) has an inner product:

\[
\langle \phi|\vartheta \rangle = \sum_{g \in G} \overline{\phi(g)}\vartheta(g)
\]

where \( \vartheta = \sum_{g \in G} \vartheta(g)|g\rangle \).

We have a similar description for \( \mathbb{C}[X] \) except that \( X \) is abelian and we use “+” to designate the group operation in \( X \). We have an inner product on \( \mathcal{H} \) (defined as for \( \mathbb{C}[G] \)) compatible with the tensor product structure. In the ensuing discussion, relevant inner products \( \langle \cdot | \cdot \rangle \) and norms \( \| \cdot \| \) induced by them will be inferred from the context.

For an element \( |u\rangle \otimes |v\rangle \) of a tensor product of vector spaces \( U, V \), we adopt
the standard notation:
\[ |u⟩|v⟩ := |u⟩ ⊗ |v⟩ ∈ U ⊗ V \]
and utilize it when it is unambiguous to do so.

First we prepare the state which is equal superposition over the group (query register) and \(|0⟩\) in the response register (omitting some details here that describe the preparation and is standard):
\[ |Ψ⟩ = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g⟩ \right) |0⟩ \quad (2.1) \]

The oracle acts by a unitary map \( O_f \) on \( ℋ \):
\[ O_f(|g⟩|y⟩) = |g⟩|y + f(g)⟩ \]

After the oracle action, the state becomes:
\[ O_f|Ψ⟩ = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g⟩|f(g)⟩ \]

We denote the resulting mixed state of the query register by \( ρ_f \):
\[ ρ_f := \text{tr}_{C[X]} \left( O_f|Ψ⟩⟨Ψ|O_f^† \right) \]
\[ = \frac{1}{|G|} \text{tr}_{C[X]} \left( \sum_{\{g,g' \in G\}} |g⟩⟨g'| ⊗ |f(g)⟩⟨f(g')| \right) \]
\[ = \frac{1}{|G|} \sum_{y \in X} \left( \sum_{\{g,g' \in G : f(g) = f(g') = y\}} |g⟩⟨g'| \right) \]

Assume the oracle hides the subgroup \( H_l \). Define the (right) coset state for \( H_l g \in H_l \setminus G \):
\[ |H_l g⟩ := \frac{1}{\sqrt{|H_l|}} \sum_{h \in H_l} |hg⟩ \]
Since \( f \) is constant and distinct on the cosets of \( H_l \), we can write:
\[ \rho_f = \frac{1}{N_f} \sum_{c \in H \setminus G} |c\rangle \langle c| \quad (2.2) \]

This state is independent of the particular function hiding the subgroup \( H_l \), and depends only on the subgroup, we may as well denote it \( \rho_l \).

\[ \rho_l = \frac{1}{N_l} \sum_{c \in H \setminus G} |c\rangle \langle c| \quad (2.3) \]

For equal prior occurrence of the subgroups, the system density operator becomes:

\[ \rho = \frac{1}{L} \sum_l \rho_l \quad (2.4) \]

Measurements to determine the subgroup \( H_l \) are described by a set of positive semidefinite operators (POVM) on \( \mathbb{C}[G] \), described by \( \{ E_k \}_{k \in \mathcal{K}} \) for some finite set \( \mathcal{K} \). This set of operators resolve the identity:

\[ \sum_k E_k = \mathbf{1}_{\mathbb{C}[G]} \]

where \( \mathbf{1}_{\mathbb{C}[G]} \) is the identity on \( \mathbb{C}[G] \). In general \( \mathcal{K} \neq \mathcal{L} \). Since the optimal measurements are in the framework of state discrimination, we assume \( \mathcal{K} = \mathcal{L} \) (decision about the subgroup \( H_l \) is based on the outcome \( l \) of a single measurement).

Given a measurement \( \{ E_l \}_{l \in \mathcal{L}} \), The probability of correctly determining a hidden subgroup is given by:

\[ S(\mathcal{E}) := \frac{1}{L} \sum_{l \in \mathcal{L}} \text{tr} (E_l \rho_l) \]

Measurement optimality is proved by using the criteria developed by Yuen, Kennedy, and Lax [19]. We have a set of states \( \{ \rho_l \}_{l \in \mathcal{L}} \) on some finite dimensional Hilbert space \( V \), indexed by a finite set \( \mathcal{L} \), and distributed according to a probability function \( \{ p_l \}_{l \in \mathcal{L}} \) such that \( p_l \) is the prior probability of occurrence of \( \rho_l \). A
measurement \( \{ E_l \}_{l \in \mathcal{L}} \) is optimal, i.e., maximizes \( S(\mathcal{E}) \) if and only if for all \( l \in \mathcal{L} \):

\[
\left( \sum_j p_j \rho_j E_j - p_l \rho_l \right) E_l = 0
\]

\[
\sum_j p_j \rho_j E_j = \sum_j p_j E_j \rho_j
\]

\[
\sum_j p_j \rho_j E_j \geq p_l \rho_l
\]

A measurement that has been useful in many applications, and proves optimal for the HSP over several groups, is called the pretty good measurement, or the PGM. The PGM, denoted by \( \mathcal{M} = \{ M_l \}_{l \in \mathcal{L}} \), is defined for the general states setting above as:

\[
M_l := p_l \rho^{-1/2} \rho_l \rho^{-1/2}, \quad \rho := \sum_{l \in \mathcal{L}} p_l \rho_l \tag{2.5}
\]

\[
\rho^{-1/2} := (\rho |_{\text{Im}(\rho)})^{-1/2} \oplus I_{\text{Ker}(\rho)}
\]

### 2.3 The single-query PGM

We begin by recapping the result of Moore and Russell [20] specialized for single-query case in which the set of subgroups are conjugates of some subgroup. Let \( H \leq G \). Denote the normalizer of \( H \) in \( G \) by \( N_G(H) \). Let the set of possible hidden subgroups \( \mathcal{S} \) be the conjugates of \( H \), \( \mathcal{S} := \{ gHg^{-1} : g \in G \} \), indexed by \( \mathcal{L} := G/N_G(H) \) (cosets of the normalizer of \( H \)). A subgroup \( H_l \in \mathcal{S} \) is some conjugate of \( H \) given by \( l \in L \). Let \( N_H := [G : H] \) and \( C_H := [G : N_G(H)] \). Let the prior probability of occurrence of any subgroup from \( \mathcal{S} \) be equal, i.e, \( 1/C_H \).

Let \( \hat{G} \) be the equivalence classes of irreducible unitary representations of \( G \), and fix a representation \( (\pi^\lambda, V^\lambda) \) in the class \( \lambda \) for each \( \lambda \in \hat{G} \). Let the dimension of \( V^\lambda \) be \( d_\lambda \). The dual representation \( (\pi^{\lambda^*}, V^{\lambda^*}) \) is given by:

\[
\langle \pi^{\lambda^*}(z)v^*, v \rangle = \langle v^*, \pi^\lambda(z^{-1})v \rangle
\]
for $z \in G$, $v \in V^\lambda$, and $v^* \in V^{\lambda^*}$.

The space $\mathbb{C}[G]$ decomposes as:

$$\mathbb{C}[G] \cong \bigoplus_{\lambda \in \hat{G}} V^{\lambda^*} \otimes V^\lambda$$

Recall the translations of $\mathbb{C}[G]$ [26]. Denote by $L$ and $R$ the left and right translation representations of $G$ on $\mathbb{C}[G]$. On the element:

$$|\phi\rangle = \sum_{g \in G} \phi(g)|g\rangle \in \mathbb{C}[G],$$

$z \in G$ acts by:

$$L(z)|\phi\rangle := \sum_{g \in G} \phi(g)|zg\rangle = \sum_{g \in G} \phi(z^{-1}g)|g\rangle$$

$$R(z)|\phi\rangle := \sum_{g \in G} \phi(g)|gz^{-1}\rangle = \sum_{g \in G} \phi(gz)|g\rangle$$

This induces corresponding actions by the computational basis $|z\rangle \in \mathbb{C}[G]$. Extend by linearity to get the left and right regular representations of $\mathbb{C}[G]$ on itself, also denoted by $L$ and $R$:

$$L, R : \mathbb{C}[G] \to \text{End}(\mathbb{C}[G])$$

With the decomposition of $\mathbb{C}[G]$, the left translation is isomorphic to:

$$L(z) \cong \bigoplus_{\lambda \in \hat{G}} \pi^{\lambda^*}(z) \otimes I_{V^\lambda}$$

and the right translation is isomorphic to:

$$R(z) \cong \bigoplus_{\lambda \in \hat{G}} I_{V^{\lambda^*}} \otimes \pi^{\lambda}(z)$$

where $I_{V^\lambda}$ and $I_{V^{\lambda^*}}$ are identity operators on the spaces $V^\lambda$ and $V^{\lambda^*}$ respectively.

Moore and Russell [20] show that the state $\rho_l$ (2.3) commutes with the right regular representation $R$ of $\mathbb{C}[G]$, and hence must be given by some element of
\( \mathbb{C}[G] \) acting by the left regular representation \( L \). By evaluating at the identity, they find that \( \rho_l \) is given by:

\[
\rho_l = \frac{1}{N_H} P_l
\]  

(2.6)

where \( P_l \) is the projection onto the space of \( H_l \)-invariants relative the left regular representation of \( \mathbb{C}[G] \).

\[
P_l = \frac{1}{|H_l|} \sum_{h \in H_l} L(h)
\]  

(2.7)

This implies that \( \rho_l \) is given by:

\[
\rho_l \cong \bigoplus_{\lambda \in \hat{G}} \rho^\lambda_l \otimes I_{V^\lambda}
\]

where:

\[
\rho^\lambda_l = \frac{1}{N_H} P^\lambda_l
\]  

(2.8)

where \( P^\lambda_l \) is the projection onto the space of \( H_l \)-invariants in \( \lambda \in \hat{G} \):

\[
P^\lambda_l = \frac{1}{|H_l|} \sum_{h \in H_l} \pi^\lambda(h)
\]  

(2.9)

\[
\rho^\lambda = \frac{1}{C_H} \sum_{l \in \mathcal{L}} \rho^\lambda_l
\]  

(2.10)

Since \( \mathcal{L} \) is the entire set of conjugates of a subgroup, it follows that \( \rho \) in (2.4) commutes with the right and the left regular representations and hence must be a scalar function of \( \lambda \in \hat{G} \), i.e., \( \rho^\lambda = c^\lambda I_{V^\lambda} \). Using this fact, the form of \( M_l \) above, and the fact that \( \text{rank}(P^\lambda_l) \) is independent of the particular subgroup \( H_l \), Moore and Russell [20] derive the PGM for the conjugate subgroups by the following
steps:

\[
\text{tr}(\rho^\lambda) = \frac{1}{CH} \sum_{i \in \mathcal{L}} \text{tr}(\rho_i^\lambda)
\]

(2.11)

\[\implies c_\lambda d_\lambda = \frac{1}{N_H} \text{rank}(P_i^\lambda)\]

\[\implies c_\lambda = \frac{1}{N_H d_\lambda \text{rank}(P_i^\lambda)}\]

\[
M_i = \frac{1}{CH} \rho^{-1/2} \rho_i \rho^{-1/2}
\]

\[\cong \bigoplus_{\lambda \in \hat{G}} M_i^{\lambda^*} \otimes I_{V^\lambda}
\]

where \(I_{V^\lambda}\) is the identity on the space \(V^\lambda\), and where:

\[
M_i^{\lambda} = \frac{1}{CH} \rho^{\lambda-1/2} \rho_i^\lambda \rho^{\lambda-1/2}
\]

(2.12)

\[
M_i^{\lambda} = \frac{d_\lambda}{CH \text{rank}(P_i^\lambda)} P_i^\lambda
\]

(assumes that \(\text{rank}(P_i^\lambda) > 0\)).

We specialize the above considerations to the case of dihedral groups. We first describe the subgroups of the dihedral group. The dihedral group, of order \(2N\), is the set:

\[
G = \{(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_N\}
\]

with the semi-direct product defined to be:

\[
(x', y') \cdot (x, y) = (x + x', (-1)^x y + y')
\]
It has the following subgroups:

\[ G \]

\[ C_k = \langle \{(0, k)\} \rangle, \text{ where } k|N \]

\[ D_{l,k} = \langle \{(0, k), (1, l)\} \rangle, \text{ where } k|N, l \in \mathbb{Z}_N \]

\[ I = \{(0, 0)\} \]

where the subgroup generated by the set \( \{g_1, g_2, \ldots\} \) is denoted by \( \langle g_1, g_2, \ldots \rangle \).

The relevance of the conjugate subgroups case to the dihedral group follows from a reduction of Ettinger and Hoyer [14]. They reduce the HSP problem of identifying an arbitrary subgroup of the dihedral group to an identification of order two subgroups of the form \( H_l := D_{l,0} = \{(0, 0), (1, l)\} \) and the trivial subgroup \( I \). Bacon et al. [21] show that the PGM is optimal in distinguishing the groups \{\( H_l \)\}. They also augment the PGM with another measurement to identify the trivial subgroup as well, but that belongs to the discussion of the multi-query case and will be mentioned there. Then for the purposes of the PGM computations, subgroups of interest are:

\[ \mathcal{S} = \{H_l : H_l = \{(0, 0), (1, l)\}, l \in \mathbb{Z}_N \} \]

The simplified problem is as follows. We have a finite set \( X \) (assume abelian). The oracle function \( f : G \rightarrow X \) has the property that \( f(hg) = f(g) \) for \( h \in H_l \) for some \( l \in \mathbb{Z}_N \), and all \( g \in G \).

Let us describe the above in terms of the models for the left translation representation of the dihedral group presented in appendix A.

\[ \mathbb{C}[G] \cong \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_N] \]
Let 

\[ g' = (x', y'), \]

then the left translation by \( g' \) on \( \gamma \otimes \varphi \) is given as:

\[ L(g') = \tau_2(g') \otimes \tau_N(g') \]  \hspace{1cm} (2.13)

\[ \tau_2(g') \gamma(x) = \gamma(x + x'), \quad \text{where} \quad \gamma \in \mathbb{C}[\mathbb{Z}_2] \]

\[ \tau_N(g') \varphi(y) = \varphi \left( (-1)^{x'} (y - y') \right), \quad \text{where} \quad \varphi \in \mathbb{C}[\mathbb{Z}_N] \]

Let \( \{ |\zeta_\nu \rangle \}_{\nu \in \mathbb{Z}_2} \) be the characters of \( \mathbb{Z}_2 \):

\[ \zeta_\nu(x) = \frac{1}{\sqrt{2}} (-1)^{\nu x}, \quad \text{where} \quad x \in \mathbb{Z}_2 \]

and \( \{ |\chi_\mu \rangle \}_{\mu \in \mathbb{Z}_N} \) be the characters of \( \mathbb{Z}_N \):

\[ \chi_\mu(y) = \frac{1}{\sqrt{N}} \omega^{\mu y}, \quad \text{where} \quad y \in \mathbb{Z}_N \]

where \( \omega = e^{2\pi i/N} \).

Under the left translation representation, \( \mathbb{C}[G] \) decomposes as:

\[ \mathbb{C}[G] = \bigoplus_{\{(\nu,\mu)\}} W^{(\nu,\mu)} \]  \hspace{1cm} (2.14)

\( W^{(\nu,\mu)} \) are the irreducible subspaces for the left translation representation.

\[ W^{(\nu,\mu)} := \mathbb{C}[\zeta_\nu] \otimes V^\mu \quad \text{if} \quad (\nu, \mu) \in \mathbb{Z}_2 \times \{0, \cdots, \lfloor N/2 \rfloor \} \]  \hspace{1cm} (2.15)

where \( \lfloor r \rfloor \) is the largest integer less than or equal to \( r \in \mathbb{R} \).

Some of the spaces \( V^\mu \) can be described simultaneously for both odd and even
These common spaces are described in terms of the character $\chi$ as:

$$V^\mu := \begin{cases} \mathbb{C}|\chi_\mu\rangle & \text{if } \mu = 0 \\ \mathbb{C}|\chi_\mu\rangle \oplus \mathbb{C}|\chi_{-\mu}\rangle & \text{if } \mu \in \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor \} \end{cases} \quad (2.16)$$

Above are all the subspaces for the case of odd $N$. When $N$ is even, there are two additional (one-dimensional) spaces coming from the character $|\chi_{N/2}\rangle$ of $\mathbb{Z}_N$:

$$V^{N/2} := \mathbb{C}|\chi_{N/2}\rangle \quad (2.17)$$

Since we are interested in the left regular representation, we can label the irreducible representations by $\{(\nu, \mu)\}$ as in (2.14). We note that under the left translation representation (2.13), the two-dimensional representations $W^{(0,\mu)} \cong W^{(1,\mu)}$, and are in the same isotypic component. $W^{(\nu,\mu)} \not\cong W^{(\nu,\mu')} \text{ for } \mu \neq \mu' \in \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor \}$ and are in different isotypic components. Denote by $L^{(\nu,\mu)}$ the restriction of left translation representation (2.13) to $W^{(\nu,\mu)}$.

$$L^{(\nu,\mu)} = L\big|_{W^{(\nu,\mu)}}$$

When $N$ is odd, $\mathcal{S}$ constitutes a single conjugacy class, so for any $H \in \mathcal{S}$, $C_H = N_H = N$. When $N$ is even, $\mathcal{S}$ is divided into two conjugacy classes corresponding to the odd and the even $l$. In that case, for any $H \in \mathcal{S}$, $C_H = N/2$, and $N_H = N$. We therefore use the equations (2.8), (2.9), and forms of (2.10), and (2.12) that do not assume that the subgroups form a single conjugacy class. We observe that the conjugate subgroup analysis above is still useful since $\mathcal{S}$ is a union of entire sets of conjugates, and we apply the method of Moore and
Russell [20] as used above (2.11) to obtain the PGM. We have the restrictions:

\[
P_l^{(\nu,\mu)} = \frac{1}{|H_l|} \sum_{h \in H_l} L^{(\nu,\mu)}(h)
\]

(2.18)

\[
\rho_l^{(\nu,\mu)} = \frac{1}{N} P_l^{(\nu,\mu)}
\]

(2.19)

\[
\rho^{(\nu,\mu)} = \frac{1}{N} \sum_{l \in \mathbb{Z}_N} \rho_l^{(\nu,\mu)}
\]

(2.20)

\[
M_l^{(\nu,\mu)} = \frac{1}{N} \rho^{(\nu,\mu)^{-1/2}} \rho_l^{(\nu,\mu)} \rho^{(\nu,\mu)^{-1/2}}
\]

(2.21)

The rank one operators \( P_l^{(\nu,\mu)} \) are given as:

\[
P_l^{(\nu,\mu)} = \left| \psi_l^{(\nu,\mu)} \right\rangle \left\langle \psi_l^{(\nu,\mu)} \right|
\]

(2.22)

with invariants common to both the odd and even \( N \) given by:

\[
|\psi_l^{(\nu,\mu)}\rangle := \begin{cases} 
|\zeta_0\rangle |\chi_0\rangle & \text{if } (\nu, \mu) = (0, 0) \\
0 & \text{if } (\nu, \mu) = (1, 0) \\
\frac{1}{\sqrt{2}} |\zeta_0\rangle (\omega^{-\mu l/2} |\chi_{\mu}\rangle + \omega^{\mu l/2} |\chi_{-\mu}\rangle) & \text{if } (\nu, \mu) \in \{0\} \times \{1, \ldots, \lfloor N/2 \rfloor \} \\
\frac{1}{\sqrt{2}} |\zeta_1\rangle (\omega^{-\mu l/2} |\chi_{\mu}\rangle - \omega^{\mu l/2} |\chi_{-\mu}\rangle) & \text{if } (\nu, \mu) \in \{1\} \times \{1, \ldots, \lfloor N/2 \rfloor \}
\end{cases}
\]

(2.23)

When \( N \) is even, the additional two invariants are dependent on \( l \) being odd or even.

When \( l \) is odd:

\[
|\psi_l^{(\nu,\mu)}\rangle := \begin{cases} 
0 & \text{if } (\nu, \mu) = (0, N/2) \\
|\zeta_1\rangle |\chi_{N/2}\rangle & \text{if } (\nu, \mu) = (1, N/2)
\end{cases}
\]

When \( l \) is even:

\[
|\psi_l^{(\nu,\mu)}\rangle := \begin{cases} 
|\zeta_0\rangle |\chi_{N/2}\rangle & \text{if } (\nu, \mu) = (0, N/2) \\
0 & \text{if } (\nu, \mu) = (1, N/2)
\end{cases}
\]
This leads to the PGM, $M_t^{(\nu,\mu)}$:

$$M_t^{(\nu,\mu)} = \begin{cases} \frac{1}{N} |\psi_t^{(\nu,\mu)} \rangle \langle \psi_t^{(\nu,\mu)}| & \text{if } (\nu, \mu) \in \mathbb{Z}_2 \times \{0\} \\ \frac{2}{N} |\psi_t^{(\nu,\mu)} \rangle \langle \psi_t^{(\nu,\mu)}| & \text{otherwise} \end{cases} \quad (2.24)$$

**Theorem.** Let $G$ be the dihedral group of order $2N$. For the HSP over the set of subgroups $\{H_l = \{(0,0),(1,l)\} : l \in \mathbb{Z}_N\}$, the standard method single-query algorithm for the Pretty Good Measurement can be implemented by using only abelian Fourier transforms. This requires $\text{poly}(\log(N))$ gates.

**Proof.** We will use two abelian quantum Fourier transforms. The first $\mathbf{H}$ (Hadamard Transform) on $\mathbb{C}[\mathbb{Z}_2]$ and the second $\mathcal{F}_N$ on $\mathbb{C}[\mathbb{Z}_N]$. Recall that

$$\mathbf{H}_\gamma(x) = \frac{1}{\sqrt{2}} \sum_{k \in \mathbb{Z}_2} \zeta_x(k) \gamma(k) = \frac{1}{\sqrt{2}} \sum_{k \in \mathbb{Z}_2} (-1)^{kx} \gamma(k)$$
$$\mathcal{F}_N \varphi(y) = \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{Z}_N} \chi_y(k) \varphi(k) = \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{Z}_N} \omega^{ky} \varphi(k)$$

We apply $\mathbf{H} \otimes \mathcal{F}_N$ to $\mathbb{C}[G]$. Consider the images of the subspaces in the direct sum decomposition of $\mathbb{C}[G]$ (2.14). For that, first, we define the image of $V^\mu$ (2.16), (2.26) under $\mathcal{F}_N$:

$$\tilde{V}^\mu := \mathcal{F}_N(V^\mu) = \begin{cases} \mathbb{C}|\mu\rangle & \text{if } \mu = 0 \\ \mathbb{C}|\mu\rangle \oplus \mathbb{C}| - \mu\rangle & \text{if } \mu \in \{1, \ldots, \lceil \frac{N-1}{2} \rceil \} \end{cases} \quad (2.25)$$

As mentioned, when $N$ is even, there are two additional (one-dimensional) spaces:

$$\tilde{V}^{\frac{N}{2}} := \mathcal{F}_N(V^{\frac{N}{2}}) = \mathbb{C}|\chi_{\frac{N}{2}}\rangle \quad (2.26)$$

Then the image of $W^{(\nu,\mu)}$ (2.15) is:

$$\tilde{W}^{(\nu,\mu)} := \mathbf{H} \otimes \mathcal{F}_N(W^{(\nu,\mu)}) = \mathbb{C}|\nu\rangle \otimes \tilde{V}^\mu \quad (2.27)$$
PGM (2.24) in the new basis is:

$$\tilde{M}_l^{(\nu,\mu)} := (H \otimes F_N) M_l^{(\nu,\mu)} (H^{-1} \otimes F_N^{-1})$$

We define:

$$|\tilde{\psi}_l^{(\nu,\mu)}\rangle := H \otimes F_N (|\psi_l^{(\nu,\mu)}\rangle), \quad (2.28)$$

Then:

$$|\tilde{\psi}_l^{(\nu,\mu)}\rangle := \begin{cases} |0\rangle|0\rangle & \text{if } (\nu,\mu) = (0,0) \\ 0 & \text{if } (\nu,\mu) = (1,0) \\ \frac{1}{\sqrt{2}} |0\rangle(\omega^{\mu l/2}|\mu\rangle + \omega^{-\mu l/2}| -\mu\rangle) & \text{if } (\nu,\mu) \in \{0\} \times \{1,\cdots, \left[\frac{N-1}{2}\right]\} \\ \frac{1}{\sqrt{2}} |1\rangle(\omega^{\mu l/2}|\mu\rangle - \omega^{-\mu l/2}| -\mu\rangle) & \text{if } (\nu,\mu) \in \{1\} \times \{1,\cdots, \left[\frac{N-1}{2}\right]\} \end{cases}$$

When \(N\) is even, the additional two invariants (transformed) are dependent on \(l\) being odd or even. When \(l\) is odd:

$$|\tilde{\psi}_l^{(\nu,\mu)}\rangle := \begin{cases} 0 & \text{if } (\nu,\mu) = (0,\frac{N}{2}) \\ |1\rangle|\frac{N}{2}\rangle & \text{if } (\nu,\mu) = (1,\frac{N}{2}) \end{cases}$$

When \(l\) is even:

$$|\tilde{\psi}_l^{(\nu,\mu)}\rangle := \begin{cases} |0\rangle|\frac{N}{2}\rangle & \text{if } (\nu,\mu) = (0,\frac{N}{2}) \\ 0 & \text{if } (\nu,\mu) = (1,\frac{N}{2}) \end{cases}$$

We express the PGM, \(\tilde{M}_l^{(\nu,\mu)}\):

$$\tilde{M}_l^{(\nu,\mu)} = \begin{cases} \frac{1}{N} |\tilde{\psi}_l^{(\nu,\mu)}\rangle\langle\tilde{\psi}_l^{(\nu,\mu)}| & \text{if } (\nu,\mu) \in \mathbb{Z}_2 \times \{0\} \\ 2|\tilde{\psi}_l^{(\nu,\mu)}\rangle\langle\tilde{\psi}_l^{(\nu,\mu)}| & \text{otherwise} \end{cases}$$

Measure the first tensor factor. Then we know \(\nu\) in the pair \((\nu,\mu)\). Since this measurement is in the computational basis of the first factor, we perform no further measurements on this factor.

We apply incomplete Von-Neumann measurements to the second factor (given
by \( \{ I_{\tilde{V}_\mu} \} \), where \( I_{\tilde{V}_\mu} \) is the identity on \( \tilde{V}^\mu \) to project the state into one of the sub-spaces \( \tilde{V}^\mu \) (2.27) for some \( \mu \), and then distinguish among the subgroups using measurements on the projected subspace.

From above, we see that we can simplify the next stage of measurement. \((\nu, \mu) = (1, 0)\) does not happen. If \((\nu, \mu) = (0, 0)\) we gain no information about the subgroup, and guess \( l \) arbitrarily. If \( N \) is even, and \((\nu, \mu) = (1, N/2)\), arbitrarily guess \( l \) to be any of the odd values and if \((\nu, \mu) = (0, N/2)\), arbitrarily guess \( l \) to be any of the even values.

Now suppose \((\nu, \mu) \in \mathbb{Z}_2 \times \{ 1, \cdots, \lfloor N/2 \rfloor \}\). The state can be written:

\[
|\tilde{\psi}_l^\mu\rangle = \begin{cases} 
\frac{1}{\sqrt{2}} (\omega^{\mu_l/2} |\mu\rangle + \omega^{-\mu_l/2} | -\mu\rangle) & \text{if } (\nu, \mu) \in \{0\} \times \{ 1, \cdots, \lfloor N/2 \rfloor \} \\
\frac{1}{\sqrt{2}} (\omega^{\mu_l/2} |\mu\rangle - \omega^{-\mu_l/2} | -\mu\rangle) & \text{if } (\nu, \mu) \in \{1\} \times \{ 1, \cdots, \lfloor N/2 \rfloor \}
\end{cases}
\]

(2.29)

In the sub-cases when \((\nu, \mu) \in \{1\} \times \{ 1, \cdots, \lfloor N/2 \rfloor \}\), we would like to eliminate the minus sign in the phase of \( |\hat{\psi}_l^\mu\rangle \) to simplify further computations. For that reason, let us define a controlled reflection (conditioned on \((\nu, \mu)\)) on \( \tilde{V}^\mu \):

\[
R^{(\nu, \mu)} := \begin{cases} 
I_{\tilde{V}_\mu} & \text{if } (\nu, \mu) \in \{0\} \times \{ 1, \cdots, \lfloor N/2 \rfloor \} \\
|\mu\rangle \langle \mu| - | -\mu\rangle \langle -\mu| & \text{if } (\nu, \mu) \in \{1\} \times \{ 1, \cdots, \lfloor N/2 \rfloor \}
\end{cases}
\]

(2.30)

where \( I_{\tilde{V}_\mu} \) is the identity on \( \tilde{V}^\mu \). This transforms \( |\tilde{\psi}_l^\mu\rangle \) to \( |\hat{\psi}_l^\mu\rangle \):

\[
|\hat{\psi}_l^\mu\rangle := R^{(\nu, \mu)} |\tilde{\psi}_l^\mu\rangle
\]

(2.31)

which have the form:

\[
|\hat{\psi}_l^\mu\rangle = \frac{1}{\sqrt{2}} (\omega^{\mu_l/2} |\mu\rangle + \omega^{-\mu_l/2} | -\mu\rangle) \quad \forall \mu \in \{ 1, \cdots, \lfloor N/2 \rfloor \}
\]

Then \( \tilde{M}_l^\mu \) transforms to \( \hat{M}_l^\mu \) defined as:

\[
\hat{M}_l^\mu := R^{(\nu, \mu)} \tilde{M}_l^\mu R^{(\nu, \mu)^{-1}}
\]
and given in terms of the invariants as:

\[ \hat{M}_l^\mu := \frac{2}{N} \langle \hat{\psi}_l^\mu | \hat{\psi}_l^\mu \rangle \]

We extend the space \( \tilde{V}^\mu \) so that the POVM’s \( \{ \hat{M}_l^\mu \} \) can be realized as projections on an orthonormal basis of an extended Hilbert space (Naimark extension).

Before describing the general case, we consider the special case when \( N \) is odd, and motivate the implementation. When \( N \) is odd, we extend \( \tilde{V}^\mu \) by embedding it into \( \mathbb{C}[\mathbb{Z}_N] \) (inclusion). First, we define an orthonormal set of states \( \{ |\Psi_l\rangle \} \in \mathbb{C}[\mathbb{Z}_N] \).

\[
|\Psi_l\rangle := \frac{1}{\sqrt{N}} \sum_{-\frac{(N-1)}{2} \leq k \leq \frac{(N-1)}{2}} \omega^{kl} |k\rangle = \sqrt{\frac{2}{N}} \hat{\psi}_l^\mu + \frac{1}{\sqrt{N}} \sum_{k \neq \pm \mu} \omega^{kl} |k\rangle
\]

We see that for any state \( |\Phi\rangle \in \tilde{V}^\mu \), considered as an element of \( \mathbb{C}[\mathbb{Z}_N] \):

\[
\langle \Psi_l | \Phi \rangle = \frac{2}{N} \langle \hat{\psi}_l^\mu | \Phi \rangle
\]

We define:

\[ \hat{M}_l := |\Psi_l\rangle \langle \Psi_l | \]

Then we map the measurement operators \( \hat{M}_l^\mu \) into \( \text{End}(\mathbb{C}[\mathbb{Z}_N]) \) as follows:

\[ \hat{M}_l^\mu \rightarrow \hat{M}_l \]

It is straightforward to check that the set \( \{ \hat{M}_l \} \) defines a measurement on \( \mathbb{C}[\mathbb{Z}_N] \).

Also, restricted to any \( \tilde{V}^\mu \), \( \{ \hat{M}_l \} \) is identical to \( \{ \hat{M}_l^\mu \} \) as a measurement. This shows that we have an orthonormal basis of the extended space \( \mathbb{C}[\mathbb{Z}_N] \), such that measurement operator \( \hat{M}_l^\mu \) in \( \tilde{V}^\mu \) is proportional to the projection on \( |\Psi_l\rangle \) in \( \mathbb{C}[\mathbb{Z}_N] \).

Now we observe that:

\[
\langle \Psi_l | \Phi \rangle = \mathcal{F}_N^{-1} \Phi(l) \frac{l}{2}
\]
This implies that the above projection, and therefore the PGM is obtained by $F_N^{-1}$ followed by measurement in the computational basis of $\mathbb{C}[\mathbb{Z}_N]$. The outcome is then $\frac{l}{2}$ with probability $\frac{2}{N}(1 - \frac{1}{2N})$.

The above part of the algorithm is dependent on the fact that 2 is invertible in $\mathbb{Z}_N$ for odd $N$. When $N$ is even (or for any $N$ in general), we modify it to work without relying on that fact. We extend $\tilde{V}^\mu$ by embedding it into $\mathbb{C}[\mathbb{Z}_{2N}]$ (inclusion). Similar to the special case of odd $N$, we define an orthonormal set of states $\{|\Psi_l\rangle\} \in \mathbb{C}[\mathbb{Z}_{2N}]$.

$$|\Psi_l\rangle = \frac{1}{\sqrt{2N}} \sum_{-N \leq k \leq (N-1)} \omega^{\frac{k}{2}} |k\rangle$$

$$= \frac{1}{\sqrt{N}} |\tilde{\psi}^\mu_l\rangle + \frac{1}{\sqrt{2N}} \sum_{k \neq \pm \mu} \omega^{\frac{k}{2}} |k\rangle$$

We see that for any state $|\Phi\rangle \in \tilde{V}^\mu$, considered as an element of $\mathbb{C}[\mathbb{Z}_{2N}]$:

$$\langle \Psi_l|\Phi\rangle = e^{i\pi\mu} \langle \Psi_{l+N}|\Phi\rangle = \sum_{y \in \mathbb{Z}_N} \overline{\Psi_l(y)} \Phi(y) = \sum_{y \in \mathbb{Z}_N} \overline{\tilde{\psi}^\mu_l(y)} \Phi(y) = \frac{1}{\sqrt{N}} \langle \tilde{\psi}^\mu_l|\Phi\rangle$$

This leads us to define the measurement embedding in the following manner (using the same notation as for the special case of odd $N$):

$$\hat{M}_l := |\Psi_l\rangle\langle \Psi_l| + |\Psi_{l+N}\rangle\langle \Psi_{l+N}|$$

We map the measurement operators $\hat{M}_l^\mu$ into $\text{End}(\mathbb{C}[\mathbb{Z}_{2N}])$ as follows:

$$\hat{M}_l^\mu \mapsto \hat{M}_l$$

Again, it is straightforward to check that the set $\{\hat{M}_l\}$ defines a measurement on $\mathbb{C}[\mathbb{Z}_{2N}]$. Also, restricted to any $\tilde{V}^\mu$, $\{\hat{M}_l\}$ is identical to $\{\hat{M}_l^\mu\}$ as a measurement.

This gives us an orthonormal basis of the extended space $\mathbb{C}[\mathbb{Z}_{2N}]$ such that measurement operator $\hat{M}_l^\mu$ in $\tilde{V}^\mu$ is proportional to projection on the subspace.
\[ C|\Psi_t\rangle \oplus C|\Psi_{t+N}\rangle \subset C[\mathbb{Z}_{2N}] \]. Now we observe that:

\[ \langle \Psi_t|\Phi \rangle = F_{2N}^{-1}\Phi(l) \]

This implies that the above projection, and therefore the PGM, is obtained by \( F_{2N}^{-1} \) followed by measurement in the computational basis of \( C[\mathbb{Z}_{2N}] \). The outcome is either \( l \) or \( l + N \) (since we know \( N \), we can find \( l \) if the latter happens) with probability \( \frac{2}{N}(1 - \frac{1}{2N}) \).

This completes our analysis of the single-query case.

### 2.4 The multi-query PGM

In this section we consider generalization of the PGM to \( k \) queries.

The system consists of \( k \) copies of \( C[G] \otimes C[X] \):

\[ \mathcal{H}^k = \bigotimes^k C[G] \otimes C[X] \]

The initial state on which the oracles act is:

\[ |\Psi^k\rangle = \bigotimes^k |\Psi\rangle \]

where \( |\Psi\rangle \) is as in (2.1). Then the state after the oracle evaluation is:

\[ \left( \bigotimes^k O_f \right) |\Psi^k\rangle = \bigotimes^k O_f |\Psi\rangle \]

Denote the mixed state conditioned on the oracle function hiding the subgroup \( H_l \) by \( \rho^k_f \).

\[ \rho^k_f = \bigotimes^k \text{tr}_{C[X]} \left( \bigotimes^k \left( O_f |\Psi\rangle\langle O_f^†| |\Psi\rangle\langle O_f^†| \right) \right) \]

\[ = \bigotimes^k \text{tr}_{C[X]} \left( O_f |\Psi\rangle\langle O_f^†| \right) \]

\[ = \bigotimes^k \rho_l \]
where $\rho_l$ is as in (2.6).

As in single-query, we notice the independence of $\rho_l^k$ from the particular function $f$, and find that it depends only on the subgroup $H_l$, so we denote the state $\rho_l^k$.

$$\rho_l^k = \bigotimes^k \rho_l$$

Relevant group for this case is the direct product of $k$ copies of $G$, $G^{\times k}$:

$$G^{\times k} = G \times G \times \cdots \times G$$

and this group acts by left and right translation on:

$$\mathbb{C}[G^{\times k}] \cong \mathbb{C}[G] \otimes \mathbb{C}[G] \otimes \cdots \otimes \mathbb{C}[G]$$

$$= \bigotimes^k \mathbb{C}[G]$$ (2.32)

Left translation action ($L^{\times k}$) by $g_0 \in G^{\times k}$ on $\vartheta \in \mathbb{C}[G^{\times k}]$ is given by:

$$L^{\times k}(g_0)\vartheta(g) = \vartheta(g_0^{-1}g), \quad \text{for } g \in G^{\times k}$$

Similarly right translation action ($R^{\times k}$) is given by:

$$R^{\times k}(g_0)\vartheta(g) = \vartheta(gg_0), \quad \text{for } g \in G^{\times k}$$

Then $\rho_l^k$ commutes with the right translation $R^{\times k}$ since each factor $\rho_l$ commutes with the right translation ($R$) on $\mathbb{C}[G]$. This implies that $\rho_l^k$ is given by an element of $\bigotimes^k \mathbb{C}[G]$ acting by the left regular representation $L^{\times k}$. In fact, by evaluating $\rho_l^k$ at the identity of $G^{\times k}$, can be expressed as:

$$\rho_l^k = \frac{1}{N_k} \bigotimes^k P_l$$

where $P_l$ is as in (4.4).

Density operator of the system, $\rho^k$, assuming uniform prior probability of oc-
P-recurrence of $H_l$ is:

$$\rho^k = \frac{1}{N} \sum_l \rho^k_l$$

Recall from (3.5) (generalized to $k$ queries), the PGM is given by a set $\{M^k_l\}$:

$$M^k_l = \frac{1}{N} \rho^{k-1/2} \rho^k \rho^{k-1/2}$$

By the results of Bacon et al. [21], PGM is optimal for the multi-query case. To identify the trivial subgroup $I$, they define the measurement operator:

$$M^k_I := I_{\otimes^k \mathbb{C}[G]} - \sum_{l \in \mathbb{Z}_N} M^k_l$$

where $I_{\otimes^k \mathbb{C}[G]}$ is the identity on $\otimes^k \mathbb{C}[G]$. Associate $M^k_I$ with the trivial subgroup. Then the expanded measurement $\{M^k_I\} \cup \{M^k_l\}_{l \in \mathbb{Z}_N}$ finds the trivial subgroup with a constant probability as long as $k \geq \log(N) + 4$. Now we come to the main result of this chapter. We give a proof by construction that there is an algorithm implementing the Pretty Good Measurement by explicitly showing the algorithm.

**Theorem 2.4.1.** Let $G$ be the dihedral group of order $2N$. For the HSP over the set of subgroups $\{H_l = \{(0,0),(1,l)\} : l \in \mathbb{Z}_N\}$, the Pretty Good Measurement for the standard method with $k$ parallel queries can be implemented by using only abelian Fourier transforms.

**Proof.** Under the left translation representation $L^* \otimes^k G$ of $G^* \otimes^k \mathbb{C}[G]$ decomposes as:

$$\otimes^k \mathbb{C}[G] = \bigotimes_{(\nu,\mu) \in \mathbb{Z}_2 \times \{0,\ldots,[N/2]\}} W^{(\nu,\mu)}$$

Let the tensor factors in (2.32) be indexed by $m \in \{1,\cdots,k\}$. Also, let $(\nu_m, \mu_m) \in \mathbb{Z}_2 \times \{0,\cdots,[N/2]\}$ index the subspaces in the tensor factor identified by $m$. Also define an ordered $k$-tuple of such pairs (represented as a vector) $\overrightarrow{(\nu,\mu)}$:

$$\overrightarrow{(\nu,\mu)} := ((\nu_1,\mu_1),\cdots, (\nu_k,\mu_k)) \in \mathbb{Z}_2 \times \{0,\cdots,[N/2]\}^k$$
By (2.14) and (2.32):

\[
\bigotimes^k \mathbb{C}[G] = \bigotimes_{m \in \{1, \cdots, k\}} \bigoplus_{(\nu_m, \mu_m) \in \mathbb{Z}_2 \times \{0, \cdots, \lfloor \frac{N}{2} \rfloor\}} W^{(\nu_m, \mu_m)}
\]

\[
= \bigoplus_{\{(\nu_1, \mu_1)\}} \cdots \bigoplus_{\{(\nu_k, \mu_k)\}} \bigotimes_{m \in \{1, \cdots, k\}} W^{(\nu_m, \mu_m)}
\]

\[
= \bigoplus_{\{(\nu, \mu)\}} \bigotimes_{(\nu_m, \mu_m) \in (\nu, \mu)} W^{(\nu_m, \mu_m)}
\] (2.33)

here \((\nu_m, \mu_m)\) is a pair from \((\nu, \mu)\).

\[
\rho^k_l = \frac{1}{N^k} \bigoplus_{\{(\nu, \mu)\}} \bigotimes_{(\nu_m, \mu_m) \in (\nu, \mu)} P_l^{(\nu_m, \mu_m)}
\]

\[
= \frac{1}{N^k} \bigoplus_{\{(\nu, \mu)\}} \bigotimes_{(\nu_m, \mu_m) \in (\nu, \mu)} |\psi_l^{(\nu_m, \mu_m)}\rangle \langle \psi_l^{(\nu_m, \mu_m)}|
\]

where \(P_l^{(\nu_m, \mu_m)}\), \(|\psi_l^{(\nu_m, \mu_m)}\rangle\) are as in (2.18) and (2.23) respectively.

From here on when we use \(m\) to index a tensor product, we assume \(m \in \{1, \cdots, k\}\). We apply the following tensor product of transforms to \(\bigotimes^k \mathbb{C}[G]\):

\[
\bigotimes^k \mathcal{H} \otimes \mathcal{F}_N
\]

By (2.33):

\[
\bigotimes^k \mathbb{C}[G] \cong \left( \bigotimes^k \mathcal{H} \otimes \mathcal{F}_N \right) \bigotimes^k \mathbb{C}[G]
\]

\[
= \bigoplus_{\{(\nu, \mu)\}} \bigotimes_{(\nu_m, \mu_m) \in (\nu, \mu)} \tilde{W}^{(\nu_m, \mu_m)}
\]
where $\bar{W}^{\mu_m,\mu_m}$ is as in (2.27). The operators $\rho^k_i$ become:

$$\hat{\rho}^k_i := \left( \bigotimes^k H \otimes F_N \right) \rho^k_i \left( \bigotimes^k H^{-1} \otimes F_N^{-1} \right) = \frac{1}{N^k} \bigoplus_{\{(\nu,\mu)\}} \bigotimes_{(\nu_m,\mu_m)\in(\nu,\mu)} \bar{\psi}_i^{(\nu_m,\mu_m)} \langle \bar{\psi}_i^{(\nu_m,\mu_m)} |$$

where $|\bar{\psi}_i^{(\nu_m,\mu_m)} \rangle$ is as in (2.28).

We define:

$$\bar{W}^{(\nu,\mu)} := \bigotimes_{(\nu_m,\mu_m)\in(\nu,\mu)} \bar{W}^{(\nu_m,\mu_m)}$$

Under an obvious isomorphism:

$$\hat{\rho}^k_i = \frac{1}{N^k} \bigoplus_{\{(\nu,\mu)\}} \bigotimes_{(\nu_m,\mu_m)\in(\nu,\mu)} \bar{\psi}_i^{(\nu_m,\mu_m)} \langle \bar{\psi}_i^{(\nu_m,\mu_m)} |$$

We also define the restriction of $\hat{\rho}^k_i$ to $\bar{W}^{(\nu,\mu)}$:

$$\hat{\rho}^k_i^{(\nu,\mu)} := \hat{\rho}^k_i \big|_{\bar{W}^{(\nu,\mu)}} = \frac{1}{N^k} \bigotimes_{(\nu_m,\mu_m)\in(\nu,\mu)} \bar{\psi}_i^{(\nu_m,\mu_m)} \langle \bar{\psi}_i^{(\nu_m,\mu_m)} |$$

Then we can express $\hat{\rho}^k_i$:

$$\hat{\rho}^k_i = \bigoplus_{\{(\nu,\mu)\}} \hat{\rho}^k_i^{(\nu,\mu)}$$

Similarly define:

$$\hat{\rho}^{k,(\nu,\mu)} := \frac{1}{N} \sum_l \hat{\rho}^k_i^{(\nu,\mu)}$$

$$\hat{M}^{k,(\nu,\mu)} := \frac{1}{N} \hat{\rho}^{k,(\nu,\mu)}^{-1/2} \hat{\rho}^k_i^{(\nu,\mu)} \hat{\rho}^{k,(\nu,\mu)}^{-1/2}$$
Then $\tilde{\rho}^k$ and $\tilde{M}_l^k$ are:

$$
\tilde{\rho}^k = \bigoplus_{\{(\nu,\mu)\}} \tilde{\rho}^{k, (\nu,\mu)} \\
\tilde{M}_l^k = \bigoplus_{\{(\nu,\mu)\}} \tilde{M}^{k, (\nu,\mu)}_l
$$

Given the decomposition of $\tilde{M}_l^k$, we perform an incomplete Von-Neumann measurement to project into one of the subspaces $\tilde{W}^{(\nu,\mu)}$. Consider the $(\nu_m, \mu_m) \in \overrightarrow{\nu, \mu}$. Suppose $N$ is even: if at least one of the $(\nu_m, \mu_m) = (1, N/2)$, then $l$ is odd, and if at least one of the $(\nu_m, \mu_m) = (0, N/2)$, then $l$ is even.

Next, assume that all of the $(\nu_m, \mu_m) \in \mathbb{Z}_2 \times \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor \}$. That means that we consider the measurement restricted to a subspace that has all of its tensor factors one of the two-dimensional subspaces.

Then, by performing the measurements on the second tensor factors in every $\tilde{W}^{(\nu_m,\mu_m)}$, our measurements are in the subspace:

$$V^{\mu} := \bigotimes_{\mu_m \in \overrightarrow{\mu}} \tilde{V}^{\mu_m}$$

(2.34)

where:

$$\mu := (\mu_m) = (\mu_1, \cdots, \mu_k) \in \{1, \cdots, \lfloor \frac{N}{2} \rfloor \}$$

Counterparts to $\tilde{\rho}^{k, (\nu,\mu)}, \tilde{\rho}^{k, (\nu,\mu)}, \tilde{M}^{k, (\nu,\mu)}_l$ are respectively:

$$
\tilde{\rho}^{k, \mu} := \frac{1}{N^k} \bigotimes_{(\mu_m) \in \mu} |\tilde{\psi}_l^{(\mu_m)}\rangle \otimes \langle \tilde{\psi}_l^{(\mu_m)}| \\
\tilde{\rho}^{k, \mu} := \frac{1}{N^{k+1}} \sum_{l} \bigotimes_{(\mu_m) \in \mu} |\tilde{\psi}_l^{(\mu_m)}\rangle \otimes \langle \tilde{\psi}_l^{(\mu_m)}| \\
\tilde{M}^{k, \mu} := \frac{1}{N} \tilde{\rho}^{k, \mu - 1/2} \tilde{\rho}^{k, \mu} \tilde{\rho}^{k, \mu - 1/2}
$$

(2.35)
where \( |\tilde{\psi}_l^{(\mu_m)}\rangle \) is as in (2.29).

At this point we apply a conditional reflection to align the phases as in the single-query case, defined as:

\[
R^{(\nu,\mu)} := \bigotimes_{(\nu_m,\mu_m) \in (\nu,\mu)} R^{(\mu_m,\mu_m)}
\]

where \( R^{(\nu,\mu)} \) is as in (2.30).

This transforms the operators \( \tilde{\rho}_k^{-}, \tilde{\rho}_k^{+} \), \( \tilde{M}_k^{-} \), \( \tilde{M}_k^{+} \) as:

\[
\hat{\rho}_k^{-} := R^{(\nu,\mu)} \tilde{\rho}_k^{+} R^{(\nu,\mu)-1} = \frac{1}{N^k} \bigotimes_{(\mu_m) \in \mu} |\tilde{\psi}_l^{(\mu_m)}\rangle \bigotimes_{(\mu_m) \in \mu} |\tilde{\psi}_l^{(\mu_m)}\rangle
\]

\[
\hat{\rho}_k^{+} := R^{(\nu,\mu)} \tilde{\rho}_k^{-} R^{(\nu,\mu)-1} = \frac{1}{N^{k+1}} \sum_l \bigotimes_{(\mu_m) \in \mu} |\tilde{\psi}_l^{(\mu_m)}\rangle \bigotimes_{(\mu_m) \in \mu} |\tilde{\psi}_l^{(\mu_m)}\rangle
\]

\[
\hat{M}_k^{-} := R^{(\nu,\mu)} \tilde{M}_k^{+} R^{(\nu,\mu)-1} = \frac{1}{N} \rho_k^{+} \tilde{\rho}_k^{-} \hat{\rho}_k^{- \frac{1}{2}}
\]

where \( |\tilde{\psi}_l^{(\mu_m)}\rangle \) is as in (2.31)

Define a \( k \)-tuple of elements from the set \( \{-1, 1\} \):

\[
\tilde{b} := (b_m) = (b_1, \cdots, b_k) \in \{-1, 1\}^k
\]

Define a scalar product pairing elements of \( \{-1, 1\}^k \) and \( \{1, \cdots, \lfloor N/2 \rfloor\}^k \):

\[
\tilde{b} \cdot \tilde{\mu} := \sum_m b_m \mu_m \pmod{2N}.
\]

then using (2.31), we have:

\[
\hat{\rho}_l^{k, \mu} = \frac{1}{(2N)^k} \sum_{\tilde{b}, \tilde{d} \in \{-1, 1\}^k} e^{\frac{i\pi (\tilde{b} \cdot \tilde{d} \cdot \tilde{\mu})}{N}} \bigotimes_{\{m\}} |b_m \mu_m\rangle \bigotimes_{\{m\}} |d_m \mu_m\rangle
\]

We make some definitions which are useful for formulating the problem. Let \( z \in \)
$\mathbb{Z}_{2N}$. First, for fixed $\vec{\mu}$ and $z \in \mathbb{Z}_{2N}$, the set of those $\vec{b}$ which result in the same sum $\vec{b} \cdot \vec{\mu} = z \pmod{2N}$:

$$C^\vec{\mu}_z := \{ \vec{b} \in \{-1, 1\}^k \mid \vec{b} \cdot \vec{\mu} = z \pmod{2N} \}$$  \hspace{1cm} (2.36)

This is a version of the subset sum problem. Stated in our context in its decision form:

**Definition 2.4.2. The subset sum problem:** given a pair $(\vec{\mu}, z) \in \{1, \cdots, [\frac{N}{2}]\}^k \times \mathbb{Z}_{2N}$, is there a sequence $\vec{b} \in \{-1, 1\}^k$ such that $\vec{b} \cdot \vec{\mu} = z \pmod{2N}$.

A pair $(\vec{\mu}, z)$ for which such a $\vec{b}$ exists is a legal instance, and $\vec{b}$ is a solution.

Accordingly, we define subspaces of $V^\vec{\mu}$ that are generated by basis elements of the form $\bigotimes_{\{m\}} |b_m\mu_m\rangle$ for $\vec{b} \in C^\vec{\mu}_z$:

$$V^\vec{\mu}_z := \bigoplus_{\vec{b} \in C^\vec{\mu}_z} \mathbb{C} \bigotimes_{\{m\}} |b_m\mu_m\rangle$$

For a fixed $\vec{\mu}$, we also have the identification:

$$\bigotimes_{\{m\}} |b_m\mu_m\rangle \leftrightarrow |\vec{b}\rangle$$

so:

$$V^\vec{\mu}_z = \bigoplus_{\vec{b} \in C^\vec{\mu}_z} \mathbb{C}|\vec{b}\rangle$$

Note that $V^\vec{\mu}$ (2.34) can be written:

$$V^\vec{\mu} = \bigoplus_{z \in \mathbb{Z}_{2N}} V^\vec{\mu}_z$$
Re-express the operator $\hat{\rho}_{l,\vec{\mu}}^{k,\vec{\mu}}$:

$$
\hat{\rho}_{l,\vec{\mu}}^{k,\vec{\mu}} = \frac{1}{(2N)^k} \sum_{\vec{b},\vec{b}' \in \{-1,1\}^k} e^{i\pi (\vec{b} \cdot \vec{\mu} - \vec{b}' \cdot \vec{\mu})} |\vec{b}\rangle \langle \vec{b}'|
$$

$$
= \frac{1}{(2N)^k} \sum_{z,z' \mid C_{\vec{\mu}}^z \neq \emptyset} e^{i\pi (z - z')/N} \left(\sum_{\vec{b} \in C_{\vec{\mu}}^z} |\vec{b}\rangle\right) \left(\sum_{\vec{b}' \in C_{\vec{\mu}}^{z'}} \langle \vec{b}'|\right) \quad (2.37)
$$

As $2N$ is even, the set of legal instances of subset sum for a particular $\vec{\mu}$: $\{z \in \mathbb{Z}_{2N} \mid C_{\vec{\mu}}^z \neq \emptyset\}$ consists of elements that are all even or all odd. This results in a simple form for $\hat{\rho}_{l,\vec{\mu}}^{k,\vec{\mu}}$:

$$
\hat{\rho}_{k,\vec{\mu}}^{k,\vec{\mu}} = \frac{1}{N} \sum_{l} \hat{\rho}_{l,\vec{\mu}}^{k,\vec{\mu}}
$$

$$
= \frac{1}{(2N)^k} \bigoplus_{\{z \mid C_{\vec{\mu}}^z \neq \emptyset\}} \left(\sum_{\vec{b} \in C_{\vec{\mu}}^z} |\vec{b}\rangle\right) \left(\sum_{\vec{b}' \in C_{\vec{\mu}}^{z}} \langle \vec{b}'|\right)
$$

We see that $\hat{\rho}_{k,\vec{\mu}}^{k,\vec{\mu}}$ is a direct sum of projections of rank 1, on the subspaces $V_{\vec{\mu}}^z$, for every $z \in \mathbb{Z}_{2N}$ such that $C_{\vec{\mu}}^z \neq \emptyset$. To accomplish the rotation needed to diagonalize $\hat{\rho}_{l,\vec{\mu}}^{k,\vec{\mu}}$ (2.37), we need the solution to the subset sum problem. Suppose there exists a method of obtaining such solutions, i.e., for every legal instance $(\vec{\mu}, z) \in \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\}^k \times \mathbb{Z}_{2N}$, one could find the set of solutions $C_{\vec{\mu}}^z$. Let $n_z$ be the cardinality of $C_{\vec{\mu}}^z$:

$$
n_z = |C_{\vec{\mu}}^z|
$$

Then by definition $V_{\vec{\mu}}^z = \mathbb{C}[C_{\vec{\mu}}^z]$.

If $n_z \neq 0$, identify the elements of $C_{\vec{\mu}}^z$ with the set $\mathbb{Z}_{n_z}$ in any order. Let the identification be given by a map (this can be seen as renumbering of $C_{\vec{\mu}}^z$):

$$
i_{\vec{\mu}}^z : \mathbb{Z}_{n_z} \leftrightarrow C_{\vec{\mu}}^z
$$

This induces an identification on the computational bases of $\mathbb{C}[\mathbb{Z}_{n_z}]$ and $\mathbb{C}[C_{\vec{\mu}}^z] = V_{\vec{\mu}}^z$ and by linearity, gives an isomorphism of these spaces, which we denote by the
Define the following transformation to $V^\vec{\mu}$:

$$T^\vec{\mu} := \iota^\vec{\mu} F_{\mathbb{Z}_n}^{-1} \quad \forall C^\vec{\mu}_z \neq \emptyset$$

where $F_{\mathbb{Z}_n}$ is the Fourier transform on $\mathbb{Z}_n$, and $I_{V^\vec{\mu}}$ is the identity on the subspace $V^\vec{\mu}$.

We apply the following direct sum of transformations to $V^\vec{\mu}$:

$$T^\vec{\mu} := \bigoplus_{\{z \mid C^\vec{\mu}_z \neq \emptyset\}} T^\vec{\mu}_z$$

This transforms $\hat{\rho}^{k,\vec{\mu}}$ (2.37) as:

$$\hat{\rho}^{k,\vec{\mu}} := T^\vec{\mu} \hat{\rho}^{k,\vec{\mu}} T^\vec{\mu}^{-1}$$

$$= \frac{1}{(2N)^k} \bigoplus_{\{z \mid C^\vec{\mu}_z \neq \emptyset\}} n_z \cdot |\iota^\vec{\mu}_z(0)\rangle \langle |\iota^\vec{\mu}_z(0)|$$

and transforms $\hat{\rho}_l^{k,\vec{\mu}}$ (2.37) as:

$$\hat{\rho}_l^{k,\vec{\mu}} := T^\vec{\mu} \hat{\rho}_l^{k,\vec{\mu}} T^\vec{\mu}^{-1}$$

$$= \frac{1}{(2N)^k} \sum_{z,z' \in \{a \mid C^\vec{\mu}_a \neq \emptyset\}} \sqrt{n_z n_{z'}} \cdot e^{i\pi(z-z')lN} |\iota^\vec{\mu}_z(0)\rangle \langle |\iota^\vec{\mu}_{z'}(0)|$$

We find that $\hat{M}_l^{k,\vec{\mu}}$ (2.35) becomes:

$$\hat{M}_l^{k,\vec{\mu}} := T^\vec{\mu} \hat{M}_l^{k,\vec{\mu}} T^\vec{\mu}^{-1}$$

$$= \frac{1}{N} \sum_{z,z' \in \{a \mid C^\vec{\mu}_a \neq \emptyset\}} e^{i\pi(z-z')lN} |\iota^\vec{\mu}_z(0)\rangle \langle |\iota^\vec{\mu}_{z'}(0)|$$

Define:

$$|\beta_l^{k,\vec{\mu}}\rangle = \frac{1}{\sqrt{N}} \sum_{\{z \mid C^\vec{\mu}_z \neq \emptyset\}} e^{i\pi z} |\iota^\vec{\mu}_z(0)\rangle$$
then:
\[ \tilde{M}_{l}^{k,\bar{\mu}} = |\beta_{l}^{k,\bar{\mu}}\rangle \langle \beta_{l}^{k,\bar{\mu}}| \]

For the last step of the algorithm, we employ a technique similar to the single-query case, with an additional prior step. First we identify the elements of the set \( \{ |\nu_{z}^{\bar{\mu}}(0)\rangle \}_{z|C_{\bar{\mu}}\neq\emptyset} \) with those of \( \mathbb{C}[\mathbb{Z}_{2N}] \) as follows:

\[ |\nu_{z}^{\bar{\mu}}(0)\rangle \leftrightarrow |z\rangle \]

Under this identification, \( |\beta_{l}^{k,\bar{\mu}}\rangle \) maps to:

\[ |\beta_{l}^{k,\bar{\mu}}\rangle \rightarrow |\tilde{\beta}_{l}^{k,\bar{\mu}}\rangle := \frac{1}{\sqrt{N}} \sum_{\{z|C_{\bar{\mu}}\neq\emptyset\}} \omega_{z}^{\bar{\mu}} |z\rangle \quad (2.38) \]

Observe that \( |\beta_{l}^{k,\bar{\mu}}\rangle \) is contained in the subspace \( Y^{k,\bar{\mu}} \subseteq \mathbb{C}[\mathbb{Z}_{2N}] \):

\[ Y^{k,\bar{\mu}} := \bigoplus_{\{z|C_{\bar{\mu}}\neq\emptyset\}} \mathbb{C}|z\rangle \quad (2.39) \]

Under the identification above, \( \tilde{M}_{l}^{k,\bar{\mu}} \) maps to:

\[ \tilde{M}_{l}^{k,\bar{\mu}} \rightarrow \tilde{M}_{l}^{k,\bar{\mu}} := |\tilde{\beta}_{l}^{k,\bar{\mu}}\rangle \langle \tilde{\beta}_{l}^{k,\bar{\mu}}| \]

We define an orthonormal set of states \( \{ |\Psi_{l}^{k}\rangle \} \in \mathbb{C}[\mathbb{Z}_{2N}] \).

\[ |\Psi_{l}^{k}\rangle := \frac{1}{\sqrt{2N}} \sum_{z\in\mathbb{Z}_{2N}} \omega_{z}^{\bar{\mu}} |z\rangle \]

\[ = \frac{1}{\sqrt{2}} |\beta_{l}^{k,\bar{\mu}}\rangle + \frac{1}{\sqrt{2N}} \sum_{\{z|C_{\bar{\mu}}\neq\emptyset\}} \omega_{z}^{\bar{\mu}} |z\rangle \]

Noticing, as before, that the set of legal instances of subset sum for a particular \( \bar{\mu}: \{ z \in \mathbb{Z}_{2N} \mid C_{z}^{\bar{\mu}} \neq \emptyset \} \) consists of elements that are all even or all odd, it follows
that for any state $\Phi \in Y^{k,\vec{\mu}}$, considered as an element of $\mathbb{C}[\mathbb{Z}_N]$:

$$
\langle \Psi^k_l | \Phi \rangle = \mp \langle \Psi^k_{l+N} | \Phi \rangle = \frac{1}{\sqrt{2}} \sum_{y \in \mathbb{Z}_N} \tilde{\beta}^k_{l,\vec{\mu}}(y) \Phi(y) = \frac{1}{\sqrt{2}} \langle \tilde{\beta}^k_{l,\vec{\mu}} | \Phi \rangle \quad (2.40)
$$

Then we map the measurement operators $\bar{M}^k_{l,\vec{\mu}}$ into $\text{End}(\mathbb{C}[\mathbb{Z}_N])$ as follows. We define:

$$
\bar{M}^k_l := |\Psi^k_l \rangle \langle \Psi^k_l | + |\Psi^k_{l+N} \rangle \langle \Psi^k_{l+N} |
$$

The map is:

$$
\bar{M}^k_{l,\vec{\mu}} \mapsto \bar{M}^k_l
$$

It is straightforward to check that the set $\{\bar{M}^k_l\}$ defines a measurement on $\mathbb{C}[\mathbb{Z}_N]$. Using (2.40), we conclude that restricted to $Y^{k,\vec{\mu}}$ (2.39), the measurement $\{\bar{M}^k_{l,\vec{\mu}}\}$ is identical to the measurement $\{\bar{M}^k_l\}$. Observe that for any $|\Theta\rangle \in \mathbb{C}[\mathbb{Z}_N]$:}

$$
\langle \Psi^k_l | \Theta \rangle = \mathcal{F}_{2N}^{-1} \Theta(l)
$$

Based on the above, the required measurement $M^k_{l,\vec{\mu}}$ is the same as performing $\mathcal{F}_{2N}^{-1}$ on $\mathbb{C}[\mathbb{Z}_N]$, followed by the measurement in the computational basis of $\mathbb{C}[\mathbb{Z}_N]$. The result is $l$ or $l+N$ (in the latter case we can determine $l$ as we know $N$) with the probability:

$$
\frac{1}{2^k N^{k+1}} \sum_{\bar{\mu} \in \mathbb{Z}_N^k} \left( \sum_{z \in \mathbb{Z}_N} \sqrt{\eta^k_{\bar{\mu}}} \right)^2
$$

Among the remaining cases, simpler of them is when at least one of the elements $\mu_m \in \overrightarrow{\mu}$ is 0. Assume that exactly one $\mu_m$ is 0 and none is $N/2$ (other cases can be reduced to this one). Similar set of calculations as above shows that this is a reduction to $k-1$ queries. We can, therefore, without loss of generality assume $\overrightarrow{\mu}$ does not contain 0 as a component.

Slight variation to the calculations cover the case when some of the components of $\overrightarrow{\mu}$ are $N/2$ (only happens when $N$ is even). We know by previous arguments that
l is odd or even. Assume that exactly one \( \mu_m \) is \( N/2 \) and none is 0 (other cases can be reduced to this one). We basically carry out the same set of transformations for the remaining \( k - 1 \) tensor factors that we did for the case when \( \vec{\mu} \) has no elements of the type 0 or \( N/2 \). The difference is that in the definition of the subset sum, (2.36), and subsequent computations, we work mod \( N \), instead of mod \( 2N \). One distinguishes between even and odd \( l \). \(|\tilde{\beta}^{k,\vec{\mu}}_l\rangle\) in (2.38) becomes (since the sum is mod \( N \)):

\[
|\tilde{\beta}^{k,\vec{\mu}}_l\rangle = \frac{1}{\sqrt{N}} \sum_{\{z : C^\vec{\mu}_z \neq \emptyset\}} \omega^{\frac{l}{2}} |z\rangle
\]

When \( l \) is even, \( l = 2t \) for some \( t \in \{0, \cdots, N/2\} \). Replacing \( l \) by \( t \), we can rewrite \(|\tilde{\beta}^{k,\vec{\mu}}_l\rangle\) as:

\[
|\tilde{\beta}^{k,\vec{\mu}}_t\rangle = \frac{1}{\sqrt{N}} \sum_{\{z : C^\vec{\mu}_z \neq \emptyset\}} \omega^{zt} |z\rangle
\]

As a result, we find that this measurement is the same as performing \( \mathcal{F}_{N}^{-1} \) on \( Y^{k,\vec{\mu}} \) (considered embedded in \( \mathbb{C}[\mathbb{Z}_N] \)), followed by measurement of \(|t\rangle\) or \(|t + N/2\rangle\) in the computational basis of \( \mathbb{C}[\mathbb{Z}_N] \). When \( l \) is odd, \( l = 2t + 1 \) for some \( t \in \{0, \cdots, N/2 - 1\} \). Replacing \( l \) by \( t \), we can rewrite \(|\tilde{\beta}^{k,\vec{\mu}}_l\rangle\) as:

\[
|\tilde{\beta}^{k,\vec{\mu}}_t\rangle = \frac{1}{\sqrt{N}} \sum_{\{z : C^\vec{\mu}_z \neq \emptyset\}} \omega^{\hat{t}} \omega^{zt} |z\rangle
\]

In this instance, before taking the inverse Fourier transform, we have to phase multiply each element \(|z\rangle\) of the basis by the corresponding \( \omega^{-\hat{t}} \) (to subtract 1 from \( l = 2t + 1 \) in the phase). The algorithm is now identical to the case of even \( l \). Apply \( \mathcal{F}_{N}^{-1} \) on \( Y^{k,\vec{\mu}} \) (considered embedded in \( \mathbb{C}[\mathbb{Z}_N] \)), and then measure \(|t\rangle\) or \(|t + N/2\rangle\) in the computational basis of \( \mathbb{C}[\mathbb{Z}_N] \).

From the construction in the proof we observe that to define the transform \( T^\vec{\mu}_z \), we need to be able to solve the subset sum problem for the particular \( \vec{\mu} \) that identifies the subspace \( V^\vec{\mu}_z \) to which the incomplete Von-Neumann measurement projects. That measurement can project into any of the \( \vec{\mu} \in \{1, \cdots, \lceil \frac{N-1}{2} \rceil \}^k \), so the general subset sum problem is to be solved with high probability and efficiently to enable us to get an efficient solution to HSP that succeeds with reasonable
probability.

This completes our analysis of the multi-query case.

2.5 The standard algorithm

We define the set of possible hidden subgroups $\mathcal{S} = \{H_l\}_{l \in \mathcal{L}}$ of $G$ indexed by a finite set $\mathcal{L}$ of cardinality $L = |\mathcal{L}|$. The probability that the oracle function hides any particular subgroup $H_l \in \mathcal{S}$ is $1/L$.

The standard method in an HSP algorithm has the following steps:

**Preparation** Starting with the Hilbert space $\mathbb{C}[G] \otimes \mathbb{C}[\mathbb{Z}_N]$, prepare a state which is an equal superposition over the group (query register $\mathbb{C}[G]$) with a $|0\rangle$ in the response register: $|\Psi\rangle = \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \right) |0\rangle$

**Query** Evaluate the oracle to get the queried state:

$$O_f |\Psi\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |f(g)\rangle |g\rangle$$

**Processing** Processing of the queried state to determine the hidden subgroup $H_l$ from the set.

1. (Optional) Measure the response register and get a coset state:

$$|H_l g\rangle = \frac{1}{\sqrt{|H_l|}} \sum_{h \in H_l} |h g\rangle \quad \text{for some } g \in G$$

2. Apply unitary transformations and perform a measurement on the query register (in the computational basis) described by a POVM $\{E_l\}_{l \in \mathcal{L}}$.

3. Based on the measurement outcome $l$, decide the hidden subgroup $H_l$. 
2.6 Single-query algorithm

The single-query algorithm starts with the coset state $|H_l g\rangle$ and comprises:

1. Apply $H \otimes F_N$ to $|H_l g\rangle$ ($F_N$ is the $N$-dimensional Fourier transform) to get $H \otimes F_N|H_l g\rangle$.

2. Measure the first tensor factor. Then we know $\nu$ in the pair $(\nu, \mu)$. Apply incomplete Von-Neumann measurements to the second factor (given by $\{I_{\tilde{V}_\mu}\}$, where $I_{\tilde{V}_\mu}$ is the identity on $\tilde{V}^\mu$) to project the state into one of the subspaces $\tilde{V}^\mu$ (2.27) for some $\mu$:

$$\tilde{V}^\mu = C|\mu\rangle \oplus C| - \mu\rangle$$
The state projects to the state:

\[
|\tilde{\psi}_l^\mu\rangle = \begin{cases} 
\frac{1}{\sqrt{2}}(\omega^{\mu l/2}|\mu\rangle + \omega^{-\mu l/2}|\mu\rangle) & \text{if } (\nu, \mu) \in \{0\} \times \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\} \\
\frac{1}{\sqrt{2}}(\omega^{\mu l/2}|\mu\rangle - \omega^{-\mu l/2}|\mu\rangle) & \text{if } (\nu, \mu) \in \{1\} \times \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\}
\end{cases}
\]

3. If \((\nu, \mu) = (0, 0)\), guess \(l\) randomly. If \(N\) is even, and if \((\nu, \mu) = (1, \frac{N}{2})\) guess \(l\) randomly to be odd, and if \((\nu, \mu) = (0, \frac{N}{2})\), guess \(l\) randomly to be even. Then return to the Preparation stage. Otherwise, \((\nu, \mu) \in \mathbb{Z}_2 \times \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\}\) and we proceed to the next step.

4. Apply a controlled reflection \(R^{(\nu, \mu)}\):

\[
R^{(\nu, \mu)} = \begin{cases} 
I_{\tilde{V}^\mu} & \text{if } (\nu, \mu) \in \{0\} \times \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\} \\
|\mu\rangle\langle\mu| - |\mu\rangle\langle-\mu| & \text{if } (\nu, \mu) \in \{1\} \times \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\}
\end{cases}
\]

where \(I_{\tilde{V}^\mu}\) is the identity on \(\tilde{V}^\mu\). This transforms \(|\tilde{\psi}_l^\mu\rangle\) to \(|\hat{\psi}_l^\mu\rangle\):

\[
|\hat{\psi}_l^\mu\rangle = \frac{1}{\sqrt{2}}(\omega^{\mu l/2}|\mu\rangle + \omega^{-\mu l/2}|\mu\rangle) \quad \forall \mu \in \{1, \cdots, \lfloor \frac{N-1}{2} \rfloor\}
\]

5. Apply \(\mathcal{F}_{2N}^{-1}\) to \(|\hat{\psi}_l^\mu\rangle\) to get:

\[
|\tilde{\phi}_l^\mu\rangle = \mathcal{F}_{2N}^{-1}(|\hat{\psi}_l^\mu\rangle) = \frac{1}{\sqrt{N}} \sum_{n \in \mathbb{Z}_2N} \cos\left(\frac{\pi \mu}{N}(n-l)\right) |n\rangle
\]

6. Measure in the computational basis to get \(l\) or \(l + N\). Return to the Preparation stage.
2.7 Multi-query algorithm

The multi-query algorithm starts with the tensor state:

\[
\bigotimes_{m=1}^{k} |\Psi\rangle \in \bigotimes_{m=1}^{k} \mathbb{C}[G] \otimes \mathbb{C}[X]
\]

where \(|\Psi\rangle\) is as in (2.1). On each tensor factor, this algorithm is identical to the single-query algorithm from section 2.6 for the first four steps. Occurrence of \((\nu_m, \mu_m) = (0,0)\) in any of the tensor factors leads to a reduction in order of the system to less than \(k\), and can be set aside without loss of generality. Also, the special cases that arise from even \(N\) are similar to the following and are not described. The case we describe is when all the \((\nu_m, \mu_m) \in \mathbb{Z}_2 \times \{1, \ldots, \left\lfloor \frac{N-1}{2} \right\rfloor\}\), which reduce to measurements involving only the second tensor components given...
by the sequences:

\[ \vec{\mu} = (\mu_m) = (\mu_1, \cdots, \mu_k) \in \{1, \cdots, [\frac{N-1}{2}] \}^k \]

on the spaces:

\[ V^{\vec{\mu}} = \bigotimes_{\mu_m \in \vec{\mu}} \tilde{V}^{\mu_m} \]

For our purposes we define:

\[ \vec{b} = (b_1, \cdots, b_k) \in \{-1, 1\}^k \]

Also define the following product (subset sum):

\[ \vec{b} \cdot \vec{\mu} = \sum_{m=1}^{k} b_m \mu_m \pmod{2N} \]

For \( z \in \mathbb{Z}_N \) define the set of \( \vec{b} \) that yield the same subset sum for the given \( \vec{\mu} \):

\[ C^\vec{\mu}_z = \{ \vec{b} \in \{-1, 1\}^k \mid \vec{b} \cdot \vec{\mu} = z \pmod{2N} \} \]

That implies that we can have \( k \) of the Single-Query Replicable Block (SQRB) from diagram in section 6 in parallel to achieve that. Next step of the algorithm takes as its input, tensor product of \( k \) SQRB outputs.

1. For the purposes of our algorithm, we can take as our starting step the production of \( k \) outputs of the SQRBs. We tensor them to get the starting state:

\[ |\hat{\psi}^{k,\vec{\mu}}\rangle = \bigotimes_{m=1}^{k} |\hat{\psi}_l^{\mu_m}\rangle = \frac{1}{(2N)^{k/2}} \sum_{z | C^\vec{\mu}_z \neq \emptyset} e^{i\pi z l/N} \left( \sum_{\vec{b} \in C^\vec{\mu}_z} \bigotimes_{m=1}^{k} |b_m \mu_m\rangle \right) \]

2. Do the identification:

\[ \bigotimes_{(m)} |b_m \mu_m\rangle \leftrightarrow |\vec{b}\rangle \]
Then the state can be written:

\[ |\hat{\psi}^{k,\vec{\mu}}\rangle = \frac{1}{(2N)^{k/2}} \sum_{z \mid C^{\vec{\mu}}_z \neq \emptyset} e^{i\pi zl/N} \sum_{\vec{b} \in C^{\vec{\mu}}_z} |\vec{b}\rangle \]

Permute \( \{\vec{b}\} \) so that for each \( z \), elements of \( \{|\vec{b}\rangle : \vec{b} \in C^{\vec{\mu}}_z\} \) are adjacent. This is where solution to **subset sum problem** is needed.

Let \( n_z = |C^{\vec{\mu}}_z| \). For each \( z \) such that \( n_z \neq 0 \), perform the following:

(a) identify the standard basis elements of \( \mathbb{C}[\mathbb{Z}_{n_z}] \) with those of \( \mathbb{C}[C^{\vec{\mu}}_z] \) with those in some fashion (renumber the elements of \( C^{\vec{\mu}}_z \)).

\[ \iota^{\vec{\mu}}_z : \{|k\rangle : k \in \mathbb{Z}_{n_z}\} \leftrightarrow \{|\vec{b}\rangle : \vec{b} \in C^{\vec{\mu}}_z\} \]

Under this identification:

\[ |\hat{\psi}^{k,\vec{\mu}}\rangle = \frac{1}{(2N)^{k/2}} \sum_{z \mid C^{\vec{\mu}}_z \neq \emptyset} e^{i\pi zl/N} \sum_{k \in \mathbb{Z}_{n_z}} \iota^{\vec{\mu}}_z |k\rangle \]

(b) Apply \( \iota^{\vec{\mu}}_z \mathcal{F}_{n_z} \iota^{\vec{\mu}}_z^{-1} \) (same as \( \mathcal{F}_{n_z} \), Fourier transform over \( \mathbb{Z}_{n_z} \), in the renumbered basis) to get:

\[ \iota^{\vec{\mu}}_z \mathcal{F}_{n_z} \iota^{\vec{\mu}}_z^{-1} |\hat{\psi}^{k,\vec{\mu}}\rangle = \sqrt{n_z} \iota^{\vec{\mu}}_z |0\rangle \]

(c) Relabel the element \( \iota^{\vec{\mu}}_z |0\rangle \) to \( |z\rangle \) (relabel \( |0\rangle \) in the previously renumbered basis to \( |z\rangle \)).

Once the above steps have been done for each \( z \) such that \( n_z \neq 0 \), the state \( |\hat{\psi}^{k,\vec{\mu}}\rangle \) has transformed to \( |\tilde{\beta}^{k,\vec{\mu}}\rangle \):

\[ |\hat{\psi}^{k,\vec{\mu}}\rangle \rightarrow |\tilde{\beta}^{k,\vec{\mu}}\rangle = \frac{1}{(2N)^{k/2}} \sum_{z \mid C^{\vec{\mu}}_z \neq \emptyset} \sqrt{n_z} e^{i\pi zl/N} |z\rangle. \]
3. Apply $\mathcal{F}_{2N}^{-1}$ to $|\overline{\beta}^k, \vec{\mu}\rangle$ to get:

$$
\mathcal{F}_{2N}^{-1}|\overline{\beta}^k, \vec{\mu}\rangle = \frac{1}{2^{(k-1)/2} \sqrt{N}} \sum_{n \in \{-N-1, \ldots, N\}} \left( \sum_{z \in \{c^k_i \neq \emptyset\}} \sqrt{n_z} \cos \frac{\pi z(n - l)}{N} \right) |n\rangle
$$

Measure in the computational basis to get $l$ or $l + N$. Return to step 1.

### 2.8 Computational complexity

The algorithm described in generality for $k$-query case, if implemented, is optimal since it is a direct implementation of the PGM. Major obstacle to such an algorithm is that the subset sum problem that occurs in identification of one-dimensional subspaces in each subspace is an NP-complete problem. This is what Bacon et al. [21] call the “quantum sampling” of solutions of the subset sum problem.

Since the Fourier transforms needed at the beginning and the end are over $\mathbb{Z}_N$ and $\mathbb{Z}_{2N}$, when $N = 2^d$ for some $d$, the Fourier transform is exact, implemented by Shor’s algorithm. For other $N$, the problem of approximating the Fourier transform [29] has been shown to be $O(n \log(n))$, where $n = \log(N)$, with an accuracy within an arbitrary inverse polynomial in $n$. Implementation of Incomplete Von-Neumann projection (a possible implementation shown in figure 2.1), conditional reflection, and phase multiplication for odd $l$ (2.41) are the other steps that are to be specified, but are known to be efficiently implementable [1]. Among other implementation issues is that the blocks in block-by-block (Fourier) transforms in step 2b of multi-query algorithm vary in size. This requires an implementation of some architecture that can accommodate this variation.

### 2.9 Conclusion and discussion

Much work has gone into the search of optimal measurements and algorithms for the HSP over semi-direct product groups. This chapter presents a mode of investigation that might be useful in approaching such problems. The work concerns
a particular family of groups, the dihedral groups. We can conceivably generalize it to other semi-direct product groups using a similar approach and ideas about measurement.

We conclude by stating that, though the problem of HSP over dihedral group is not solved efficiently in this chapter, nevertheless, we have found an interesting approach to the implementation of an optimal measurement for the standard method in HSP.
Chapter 3

Single-query optimization

As described in the Chapter 1, an equal superposition query with \(|0\rangle\) in the response register is used in the “standard method” of single-query algorithms for the hidden subgroup problem (HSP). It is not, however, necessary to work with the standard query. To depart from it, we have to give some structure to the response space (codomain of the oracle function) while being consistent with the HSP definition. We assume the response space is a finite abelian group, an assumption frequently made in the literature and one that has connections to some important examples including the reduction by Regev [5] of the unique shortest vector problem (Unique-SVP). During the course of this part of the research, we generalize the problem of optimal query search by including optimization over queries, extending the previous paradigm of state discrimination with respect to measurements alone. We include all the queries which are equal superposition in the query register and arbitrary in the response register: \(\frac{1}{\sqrt{|G|}}(\sum_{g \in G} |g\rangle) \otimes |s\rangle\), the “equal superposition tensor product” (ESTP) queries. We introduce a different query from among ESTP queries, the “character query”. It generalizes the well-known phase kickback trick from one of the earliest quantum algorithms due to Deutsch and Jozsa [23], which solves in one query the question of whether a function from \(\mathbb{Z}_2\) to itself is constant or not. The character query maximizes the success probability of subgroup identification under a uniform prior, for the HSP in which the oracle functions take values in a finite abelian group.

This novel approach improves the existing performance of the algorithms of its
kind, and has connections to some important work in optimal measurements that precedes it [22]. It explains in a representation theoretic way the simple case of Deutsch-Jozsa algorithm. We also consider another example that has been studied by other researchers and has connection to HSP over various groups. This is when the subgroups are drawn from a set of conjugate subgroups. We use the result on common optimal measurements to find a success probability higher than previously found by Moore and Russell [20] for the standard method.

3.1 Introduction

3.1.1 The phase kickback trick

The Deutsch-Jozsa algorithm [23,30] is one of the earliest examples of quantum algorithms. It determines if a function \( f : \mathbb{Z}_2^\times \rightarrow \mathbb{Z}_2 \) is constant or “balanced” (0 on exactly half of the domain). The phase kickback trick [31] version of the algorithm solves the problem with one oracle query. Its underlying problem (Deutsch’s problem) for single bit \((n = 1)\) is an instance of the hidden subgroup problem (HSP). Being a basic example, it provides a good motivation for the rest of the discussion and a chance to familiarize the reader with some concepts and definitions that will come up.

We follow the path in [30] to recall the algorithm and compare the “standard method” (as defined in [16]) with the “phase kickback trick”.

We are given an oracle \( O_f \) that implements the function \( f \) as a unitary transformation on \( \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_2] \):

\[
O_f : |x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle
\]

The first qubit on which the oracle evaluates the function \( f \) is the “query register”, and the second qubit to which the oracle evaluation is added is the “response register”.

In both the methods, the initial state, or the “query”, is of the form: \( |\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|v\rangle \). In the standard method for Deutsch’s problem \( |v\rangle \) is set to \( |0\rangle \).
In the phase kickback trick $|v\rangle$ is set to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. It is this response register part, $|v\rangle$, of the query that we will refer to as the “slate” of the query. Let us write the two queries.

$$|\Psi_s\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$$  \hspace{1cm} \text{(the standard query)}

$$|\Psi_p\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$  \hspace{1cm} \text{(the phase kickback query)}

Recall the Hadamard transform $H$, Fourier transform on $\mathbb{Z}_2$. Its action on the computational basis is:

$$H: \begin{cases} |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =: |+\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |-\rangle \end{cases}$$

Rewrite the queries in terms of $|+\rangle$ and $|-\rangle$:

$$|\Psi_s\rangle = |+\rangle|0\rangle$$

$$|\Psi_p\rangle = |+\rangle|-\rangle$$

In the standard method, the state after the oracle evaluation is:

$$O_f|\Psi_s\rangle = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle) + \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)|-\rangle \quad (3.1)$$

whereas for the phase kickback trick, the state after oracle evaluation is:

$$O_f|\Psi_p\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)|-\rangle \quad (3.2)$$

Next is the measurement. Consider the state $O_f|\Psi_s\rangle$ arising from oracle evaluation on the standard query first. An application of the Hadamard transform $H$ to each register (denoted by $H \otimes H$), rotates the state to:

$$H \otimes H (O_f|\Psi_s\rangle) = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{2\sqrt{2}}\left[ ( (-1)^{f(0)} + (-1)^{f(1)} |0\rangle \\
+ (-1)^{f(0)} - (-1)^{f(1)} |1\rangle \right]|1\rangle$$

Measure the response (second) register. If the result is 0, which occurs with prob-
ability $1/2$, there is no information about the function. Output either “constant” or “balanced” (random guess), which would be correct with probability $1/2$. If the result is 1, then measure the query (first) register. If the result is 0, output “constant”. If the result is 1, output “balanced”. With overall probability $3/4$ we get the correct answer.

Note that we can work solely with the query register to get the same result through a slightly different route. Apply $H$ to the query register (denoted by $H \otimes I$, where $I$ is the identity operator on $\mathbb{C}[\mathbb{Z}_2]$).

$$H \otimes I (O_f |\Psi_s\rangle) = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} \left[ ((-1)^{f(0)} + (-1)^{f(1)}) |0\rangle + ((-1)^{f(0)} - (-1)^{f(1)}) |1\rangle \right] |\pm\rangle$$

Measure the query register and output “constant” if the result is 0, otherwise output “balanced”. The algorithm succeeds with overall probability $3/4$ as before. So instead of making measurements on both the registers, we may as well just measure the query register.

Now consider the state after oracle evaluation on the phase kickback query, $O_f |\Psi_p\rangle$. Apply $H$ to the query register.

$$H \otimes I (O_f |\Psi_p\rangle) = \frac{1}{2} \left[ ((-1)^{f(0)} + (-1)^{f(1)}) |0\rangle + ((-1)^{f(0)} - (-1)^{f(1)}) |1\rangle \right] |\pm\rangle$$

Measure the query register. If the result is 0, output “constant”, otherwise output “balanced”. With probability 1 we get the correct answer. The measurement is the same for both the methods and is confined to the query register. This measurement (including the Hadamard transform) of the query register is what we refer to as the “measurement for Deutsch’s problem”. It can also be described as the measurement in the basis $\{|+, |\pm\rangle\}$ (without the Hadamard transform) of the query register. If the result is $|+\rangle$, output “constant”. If the result is $|\pm\rangle$, output “balanced”.

This calculation is used to compare the probability of success of the two queries in identifying the function as being constant or balanced. While demonstrating that, it raises the question of how in general would one be able to derive such a
query. We approach the problem from the perspective of query search.

### 3.1.2 The hidden subgroup problem and the state discrimination approach

Let us recall the general hidden subgroup problem as stated in [15].

**Hidden Subgroup Problem (HSP)** Let $G$ be a group, $X$ a finite set, and $f : G \to X$ a function. There exists a subgroup $H \leq G$ such that $f$ is constant and distinct on the cosets (assume left cosets) of $H$. That is, the function has the property:

$$f(gh) = f(g) \quad \forall h \in H, \ g \in G$$

and $f(g) = f(g') \iff g' \in gH$. $f$ is accessed via queries to an oracle. Using information gained from evaluations of $f$ via its oracle, determine a generating set for $H$.

We say that the function $f$ hides the subgroup $H$, and the oracle implements the function $f$. We call $X$ the “response space”, $\mathbb{C}[G]$ the “query register” and $\mathbb{C}[X]$ the “response register”. Together they form the system $\mathbb{C}[G] \otimes \mathbb{C}[X]$ on which the oracle and measurement act.

Within the standard method, optimal measurements have been determined in many cases using results from the state discrimination approach. In this paradigm, a measurement is deemed optimal if it maximizes the probability of subgroup identification over some set of subgroups of $G$ distributed according to a (usually uniform) prior probability. Optimality can be confirmed by verifying simple checkable criteria due to Holevo [18], and Yuen, Kennedy, and Lax [19]. This technique has been shown to be very useful [20–22] in works investigating optimal measurements.

In state discrimination, the objects to be distinguished are a set of states $\{\rho_k\}_{k \in \mathcal{K}}$ on some finite dimensional Hilbert space $V$, indexed by a finite set $\mathcal{K}$, and distributed according to a probability function $\{p_k\}_{k \in \mathcal{K}}$ such that $p_k$ is the prior probability of occurrence of $\rho_k$. A measurement on $V$ is described by a set of operators (POVM) $\mathcal{E} := \{E_k\}_{k \in \mathcal{K}}$. These satisfy: $E_k \geq 0$ and $\sum_{k \in \mathcal{K}} E_k = I$, where $I$ is the identity operator. The measurement operator $E_k$ corresponds to
the outcome \( k \), associated to the state \( \rho_k \). The probability of successful state discrimination using a measurement \( \mathcal{E} = \{ E_k \}_{k \in \mathcal{X}} \) is:

\[
S(\mathcal{E}) := \sum_{k \in \mathcal{X}} p_k \text{ tr} (E_k \rho_k)
\]

The idea is to find a measurement that maximizes \( S(\mathcal{E}) \) over the set of all measurements. Such a measurement is deemed optimal.

In Deutsch’s problem for single bit, the relevant HSP is as follows. The group \( G = \mathbb{Z}_2 \). The response space is \( X = \mathbb{Z}_2 \). Possible hidden subgroups are: \( H_0 := G \) and \( H_1 := \{0\} \). Constant functions hide the subgroup \( H_0 \) and balanced functions hide \( H_1 \). The system is:

\[
\mathcal{H} := \mathbb{C}[G] \otimes \mathbb{C}[X] = \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_2]
\]

State of the system after querying the oracle implementing a function \( f \) in the standard method is given by (3.1). Since we are interested in measurements on the query register \( \mathbb{C}[G] \), we need only consider the reduced density operator for the query register, as shown in Nielsen and Chuang [1]. This is found by taking the partial trace over the response register \( \mathbb{C}[X] \):

\[
\text{tr}_{\mathcal{X}} \left( O_f |\Psi_s \rangle \langle \Psi_s | O_f^\dagger \right).
\]

If \( f \) is constant, i.e., hides \( H_0 \), the mixed state (reduced density operator on the query register) is:

\[
\rho_{s_0} := |+\rangle \langle +|
\]

If \( f \) is balanced, i.e., hides \( H_1 \), the mixed state is:

\[
\rho_{s_1} := \frac{1}{2} (|+\rangle \langle +| + |−\rangle \langle −|)
\]

Bacon and Decker [22] derive the optimal measurement for the standard method single-query HSP for a finite group \( G \), assuming that there is a uniform prior probability on the set of all subgroups of \( G \) of being hidden by the oracle function. To underscore the issue, they show at the outset that the aptly named Pretty Good Measurement (PGM) [20], which is optimal in this sense for several important cases, is sub-optimal for Deutsch’s problem. The PGM, denoted by
$\mathcal{M} = \{M_k\}_{k \in \mathcal{X}}$, for the general states setting is defined as:

$$M_k := p_k \rho_k^{-1/2}\rho p^{-1/2}, \quad \rho := \sum_{k \in \mathcal{X}} p_k \rho_k$$

$$\rho^{-1/2} := (\rho|\text{Im}(\rho))^{-1/2} \oplus I_{\text{Ker}(\rho)} \quad (3.5)$$

For Deutsch’s problem using the standard method with the assumption of uniform prior probability on the subgroups, the PGM, denoted by $\mathcal{M}_s = \{M_{s_0}, M_{s_1}\}$, becomes:

$$M_{s_0} = \frac{2}{3}|+\rangle\langle+| \quad \text{and} \quad M_{s_1} = \frac{1}{3}|+\rangle\langle+| + |−\rangle⟨−|$$

which has the success probability $S_d = 2/3$ by (3.4), less than the $3/4$ obtained by the standard method above. The measurement for Deutsch’s problem (defined in section 3.1.1 as the measurement on the query register for both the standard method and the phase kickback trick) written as a POVM, is:

$$E_0 := |+\rangle\langle+| \quad \text{and} \quad E_1 := |−\rangle⟨−|$$

Let us take a look at the phase kickback trick for Deutsch’s problem, and compute the mixed states for this case using (3.2). If $f$ is constant, i.e., hides $H_0$, the mixed state is:

$$\rho_{p_0} := |+\rangle\langle+|$$

If $f$ is balanced, i.e., hides $H_1$, the mixed state is:

$$\rho_{p_1} := |−\rangle⟨−|$$

It is apparent that the PGM, denoted by $\mathcal{M}_p = \{M_{p_0}, M_{p_1}\}$, for this set of mixed states is given by:

$$M_{p_0} = |+\rangle\langle+| = E_0 \quad \text{and} \quad M_{p_1} = |−\rangle⟨−| = E_1$$

which is the measurement for Deutsch’s problem, yielding a success probability of 1, certainly optimal. This contrasts with the standard method for which the
PGM was found to be sub-optimal. By definition, the PGM depends on the set of mixed states to be distinguished, which in turn depends both on the possible subgroup that the oracle hides and the query presented to the oracle. The question of optimality of the PGM, or for that matter any measurement, is perhaps better posed in that context. It is interesting that the particular measurement $M_p$ which is optimal for the phase kickback query also works well for the standard query and is in fact optimal. We can verify this by the construction of Bacon and Decker [22], or by the checkable optimality conditions of Yuen, Kennedy, and Lax [19]. Under some assumptions, we find that a wider set of queries have shared optimal measurements.

### 3.1.3 Query search

We build upon the paradigm of state discrimination hitherto adopted. Much of the literature on the subject considers HSP for a finite group $G$. This is also what we assume. We impose no restrictions on the set of possible hidden subgroups, letting that set be some arbitrarily chosen set of subgroups of $G$. We work with the following reasonable assumptions: there is a uniform prior probability on the given set of subgroups of being hidden by the oracle function, and similarly there is a uniform prior probability that the oracle implements a function from the set of functions hiding a particular subgroup. The former is granted in [20–22], and the latter is within the spirit of the HSP where the value of a function gives no information about the hidden subgroup. Although in the definition of the HSP, the response space $X$ can be any finite set, in the literature and the instances with which we are familiar, it is some abelian group of finite cardinality. For example, Regev [5] takes advantage of this structure in his reduction of the unique shortest vector in a lattice problem (Unique-SVP) to HSP over the dihedral group. Having this structure on $X$ allows us to look for ways in which it can be exploited to enhance the success probability of an HSP algorithm. It is consistent with the oracle action definition for the general HSP. We consider the queries that are in an equal superposition state over the group and arbitrary in the slate (state of the response register $\mathbb{C}[X]$), referring to these as the equal superposition tensor.
product or ESTP queries. We consider algorithms in which the measurements are restricted to the query register $\mathbb{C}[G]$.

Previous works [20–22] investigating the optimality of measurements for the standard method have used the maximization of the probability of subgroup identification as a criterion. We extend the criterion of optimality to ESTP queries: to be optimal, a query need maximize the probability of subgroup identification over all measurements and over all ESTP queries. It turns out that a generalization of the query used for phase kickback has the highest success probability. We call such a query a “character query”: its slate is a particular character of $X$.

In section 3.2 we describe the context, explicitly state the assumptions and the class of algorithms to be used, and review some background material. In section 3.3 we motivate and develop the main result concerning the mixed state obtained after the oracle evaluation on a query, assuming the oracle hides a particular subgroup. Perhaps somewhat curiously, this state does not depend on which abelian group $X$ is, and depends only on its cardinality, i.e., the dimension of the response register. In section 3.4 we give definitions of the “standard query” and the “character query”. We find that any measurement can be taken to be an element of the group algebra $\mathbb{C}[G]$ acting by the right regular representation. Further, the success probability of any query is linearly dependent on that of the character query. More importantly, besides the phase multiples of a constant query, all ESTP queries have identical optimal measurements. This allows us to reuse previously known optimal measurements, specially those from the vast literature on the standard query based HSP. In section 3.5 we prove that the character query has the maximum probability of success, and does strictly better than the standard query. This gives us an explicit example of a query that satisfies our optimality criterion. We then take another look at the Deutsch’s problem for single bit. In the process we re-explain why phase kickback works as well as it does for Deutsch’s problem in the single bit case from a representation theory point of view, with a clue to other problems in the HSP category. In section 3.6 we derive the success probability when the family of subgroups consists of conjugates. We find an improvement over the success probability found by Moore and Russell [20], and describe how this case contrasts
with Deutsch’s problem. Section 3.7 is the conclusion and discussion section.

3.2 Background

To begin, we define some terms that are relevant to this discussion. We have the following data: a finite group $G$, a set $\mathcal{S} = \{H_k\}_{k \in \mathcal{K}}$ of subgroups of $G$ indexed by a finite set $\mathcal{K}$ of cardinality $K := |\mathcal{K}|$. For a subgroup $H_k \in \mathcal{S}$, we denote its index by $N_k := [G : H_k]$. The probability that the oracle function hides any particular subgroup $H_k \in \mathcal{S}$ is $1/K$.

We fix the response space $X$ to be some finite abelian group. Up to isomorphism, we can assume that $X = \mathbb{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbb{Z}_{p_m^{\alpha_m}}$ for some primes $p_i$ and some $m, \alpha_i \in \mathbb{N}_{>0}$. Let $D := |X|$. Then $D = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$. By necessity $D \geq \max_{k \in \mathcal{K}} \{N_k\}$. Associated with each subgroup $H_k \in \mathcal{S}$, we have the set $\mathcal{F}_k$ of all the oracle functions that satisfy condition (3.3) for the subgroup $H_k$.

$$\mathcal{F}_k := \{f : G \to X : f \text{ is constant and distinct on the left cosets of } H_k\}$$

The probability that the oracle implements a function $f \in \mathcal{F}_k$ given that the function hides the subgroup $H_k$ is $1/|\mathcal{F}_k|$.

We have a Hilbert space, $\mathcal{H}$, describing the composite system. It is the tensor product of the query register: $\mathbb{C}[G]$, and the response register: $\mathbb{C}[X]$.

$$\mathcal{H} := \mathbb{C}[G] \otimes \mathbb{C}[X]$$

We introduce the computational basis of $\mathbb{C}[G]$ consisting of the $\delta$ functions:

$$\delta_z(g) = \begin{cases} 1, & g = z \\ 0, & \text{otherwise} \end{cases}$$

We also write $|z\rangle := \delta_z$. Then an element $|\phi\rangle \in \mathbb{C}[G]$ has a unique expression as a sum $|\phi\rangle = \sum_{g \in G} \phi(g)|g\rangle$. 

\[ \langle \phi | \vartheta \rangle = \sum_{g \in G} \overline{\vartheta(g)} \vartheta(g) \]

where \( \vartheta = \sum_{g \in G} \vartheta(g) \, |g \rangle \).

We remind ourselves of translations of \( \mathbb{C}[G] \) [26]. We denote by \( L \) and \( R \) the left and right translation representations of \( G \) on \( \mathbb{C}[G] \). On the element:

\[ |\phi\rangle = \sum_{g \in G} \phi(g) |g\rangle \in \mathbb{C}[G], \]

\( z \in G \) acts by:

\[ L(z)|\phi\rangle := \sum_{g \in G} \phi(g) |zg\rangle = \sum_{g \in G} \phi(z^{-1}g) |g\rangle \quad (3.6) \]

\[ R(z)|\phi\rangle := \sum_{g \in G} \phi(g) |gz^{-1}\rangle = \sum_{g \in G} \phi(gz) |g\rangle \quad (3.7) \]

This induces corresponding actions by the computational basis \( |z\rangle \in \mathbb{C}[G] \). Extend by linearity to get the left and right regular representations of \( \mathbb{C}[G] \) on itself, also denoted by \( L \) and \( R \):

\[ L, R : \mathbb{C}[G] \rightarrow \text{End}(\mathbb{C}[G]) \]

We have a similar description for \( \mathbb{C}[X] \) except that \( X \) is abelian and we use “+” to designate the group operation in \( X \). We have an inner product on \( \mathcal{H} \) (defined as for \( \mathbb{C}[G] \)) compatible with the tensor product structure. In the ensuing discussion, relevant inner products \( \langle \cdot | \cdot \rangle \) and norms \( ||\cdot|| \) induced by them will be inferred from the context.

An oracle implementing a function \( f \) is described by the unitary operator \( O_f \) which acts on a basis state \( |g\rangle \otimes |y\rangle \in \mathcal{H} \) by:

\[ O_f : |g\rangle \otimes |y\rangle \mapsto |g\rangle \otimes |y + f(g)\rangle \]

Hence oracle evaluation of \( f \) on the state of the query register \( \mathbb{C}[G] \) is added to
Definition 3.2.1. A query is a unit norm state in $\mathcal{H}$, presented to the oracle for evaluation. The set of queries is then: $\{ |\Psi\rangle \in \mathcal{H} : \| |\Psi\rangle \| = 1 \}$.

Queries of interest to us are assumed to be in an equal superposition state over the group but arbitrary in the response register. We refer to them as the equal superposition tensor product (ESTP) queries. Denote this class of queries $Q_0 \subset \mathcal{H}$.

$$Q_0 := \{ \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v\rangle : |v\rangle \in \mathbb{C}[X], \| |v\rangle \| = 1 \}$$

We restrict the algorithms to those comprising the following steps:

(i) Prepare a query $|\Psi\rangle \in Q_0$.

(ii) Evaluate the oracle on $|\Psi\rangle$.

(iii) Measure the query register using a measurement (POVM) $\mathcal{E} = \{ E_k \}_{k \in \mathcal{K}}$.

Observe the outcome $k$ and decide upon the corresponding $H_k \in \mathcal{S}$ as the hidden subgroup.

A query $|\Psi\rangle = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v\rangle \in Q_0$ is determined by the tensor factor $|v\rangle \in \mathbb{C}[X]$. This prompts the definition of a slate.

Definition 3.2.2. Let $|\Psi\rangle = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v\rangle$ be an ESTP query. Its response register part $|v\rangle$ is the slate of the query $|\Psi\rangle$.

We define the set of slates $S_0 := \{ |v\rangle \in \mathbb{C}[X] : \| |v\rangle \|_X = 1 \}$. By definition, $S_0$ can be identified with $Q_0$:

$$\iota_{S_0} : S_0 \leftrightarrow Q_0, \quad |v\rangle \mapsto \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v\rangle \quad (3.8)$$

Given this identification, we will refer to queries $|\Psi\rangle = \iota_{S_0} |v\rangle = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v\rangle$ by their slate $|v\rangle$ and vice versa.
We recall the Fourier transform on $X$:

$$\mathcal{F}_X : |y\rangle \mapsto \frac{1}{\sqrt{D}} \sum_{x \in X} \omega^{xy} |x\rangle =: |\chi_y\rangle$$

(3.9)

where $y = (y_j), x = (x_j) \in X$, $\omega = (\omega_j)$, $\omega_j = e^{i2\pi j/p}$ and $\omega^{xy} = \omega^{y_1 x_1} \cdots \omega^{y_m x_m}$.

A slate $|v\rangle$ can be written in terms of the characters, $|\chi_y\rangle$, of $X$.

$$|v\rangle = \sum_{y \in X} \beta_{v,y} |\chi_y\rangle \quad \text{where} \quad \beta_{v,y} := \langle \chi_y | v \rangle$$

(3.10)

### 3.3 Subgroup states

States arising from functions $f \in \mathcal{F}_k$ (constant and distinct on the left cosets of $H_k$) are in some sense described by the same subgroup $H_k$ and a reasonable measurement should target that subgroup. Before we make this precise, let us consider the state after the oracle implementing some function $f$ (not necessarily in $\mathcal{F}_k$) has acted on a query $|\Psi\rangle = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v\rangle \in Q_0$.

$$O_f|\Psi\rangle = \sum_{y \in X} \beta_{v,y} \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} \omega^{-y,f}(g) |g\rangle \right) \otimes |\chi_y\rangle$$

where $\{\beta_{v,y}\}_{y \in X}$ are as in (3.10). We denote the mixed state of the query register by $\rho_{f,v}$:

$$\rho_{f,v} := \text{tr}_{\mathbb{C}[X]} \left( O_f |\Psi\rangle \langle \Psi | O_f^\dagger \right)$$

$$= \frac{1}{|G|} \sum_{y \in X} |\beta_{v,y}|^2 \left( \sum_{g,g' \in G} \omega^{-y,f(g)-f(g')} |g\rangle \langle g'| \right)$$

(3.11)

Recall the definition of a measurement as relevant to our discussion. A measurement (POVM) on the query register $\mathbb{C}[G]$ is described by a set of operators $\mathcal{E} := \{E_k\}_{k \in \mathcal{K}}$ where $E_k \in \text{End}(\mathbb{C}[G])$ and satisfy:

(i) $E_k \geq 0 \ \forall k \in \mathcal{K}$

(ii) $\sum_{k \in \mathcal{K}} E_k = I$
Here \( \mathbf{I} \) is the identity operator on \( \mathbb{C}[G] \).

If the state of the query register is given by a density operator \( \rho_G \in \text{End}(\mathbb{C}[G]) \), then the outcome \( k \in \mathcal{K} \) is observed with probability \( \text{tr}(E_k \rho_G) \). By choice, the measurement operator \( E_k \) is associated with the subgroup \( H_k \), so that a measurement outcome \( k \) corresponds to the subgroup \( H_k \).

Given a state \( |v\rangle \) and an oracle implementing the function \( f \), the mixed state of the query register \( \mathbb{C}[G] \) after oracle evaluation is \( \rho_{f,v} \) (3.11). The probability of observing the outcome \( k' \) is \( \text{tr}(E_{k'} \rho_{f,v}) \). Now assume that the oracle hides the subgroup \( H_k \). Since all the \( f \in \mathcal{F}_k \) are assumed equally likely, the probability of outcome \( k' \) given that the oracle hides the subgroup \( H_k \), is described by the following probability function:

\[
\mu_{v,E}(k'|k) := \frac{1}{|\mathcal{F}_k|} \sum_{f \in \mathcal{F}_k} \text{tr}(E_{k'} \rho_{f,v}) = \text{tr} \left( E_{k'} \frac{1}{|\mathcal{F}_k|} \sum_{f \in \mathcal{F}_k} \rho_{f,v} \right)
\]

This leads us to the following notion:

**Definition 3.3.1.** A subgroup state for the subgroup \( H_k \) and slate \( |v\rangle \) is a mixed state, obtained by averaging \( \{\rho_{f,v}\}_{f \in \mathcal{F}_k} \) from (3.11). Denote this state \( \rho_{k,v} \).

\[
\rho_{k,v} := \frac{1}{|\mathcal{F}_k|} \sum_{f \in \mathcal{F}_k} \rho_{f,v} \tag{3.12}
\]

\( \mu_{v,E}(k'|k) \) can be written as a function of the subgroup state as:

\[
\mu_{v,E}(k'|k) = \text{tr}(E_{k'} \rho_{k,v}) \tag{3.13}
\]

A subgroup state aggregates the mixed states resulting from oracle functions hiding a particular subgroup into a single mixed state. A measurement aims to distinguish such subgroup states.

To be able to work with oracle functions, however, we must make a few identifications. By definition, an oracle function \( f \in \mathcal{F}_k \), hiding the subgroup \( H_k \in \mathcal{S} \), factors through quotient by \( H_k \). Denote the quotient map by \( q_k \) (fixed by the
choice of $k \in \mathcal{K}$).

$$q_k : G \rightarrow G/H_k, \quad g \mapsto gH_k$$

To enumerate the various sets consistently, we can identify $X$ with the set

$$\{0, \ldots, D - 1\} \subset \mathbb{N}$$
as follows:

$$\iota_X : X \leftrightarrow \{0, \ldots, D - 1\}, \quad x = (x_j) \mapsto \sum_{j=1}^{m} x_j \prod_{i=1}^{j-1} p_i^{a_i}$$

For $n \in \{0, \ldots, D - 1\}$, define the set of “first $n$ elements in $X$”:

$$X_n := \iota_X^{-1}(\{0, \ldots, n - 1\})$$

For each $k \in \mathcal{K}$, we can identify the cosets $G/H_k$ with $X_{N_k}$. Fix such an identification $\iota_k$.

$$\iota_k : X_{N_k} \leftrightarrow G/H_k \quad (3.14)$$

With these constructions in hand, $f \in \mathcal{F}_k$ can be written as a composition:

$$f = \tilde{f}_k \circ q_k = \gamma \circ \iota_k^{-1} \circ q_k \quad (3.15)$$
as shown in figure 3.1, where $\tilde{f} : G/H_k \rightarrow X$ and $\gamma : X_{N_k} \rightarrow X$ are the unique maps such that the diagram commutes.

$$G \xrightarrow{q_k} G/H_k \xrightarrow{\iota_k^{-1}} X_{N_k}$$

Figure 3.1: Oracle function $f$ factors

It is then immediate that $\gamma$ is injective. As $X_{N_k} \subseteq X$, $\gamma$ is also the restriction of some permutation of $X$ to $X_{N_k}$. Let the set of such restrictions be given by the
set $\Gamma_k$.

$$\Gamma_k := \{ \sigma | x_{N_k} : \sigma \in S_X \}$$

(3.16)

Denote by $S_X$ the group of permutations of $X$. Then for each $\gamma \in \Gamma_k$, the set:

$$S_\gamma := \{ \sigma \in S_X : \sigma | x_{N_k} = \gamma \}$$

(3.17)

has cardinality $(D - N_k)!$. Since such sets partition $S_X$, the number of possible oracle functions $f \in \mathcal{F}_k$ for every subgroup $H_k \in \mathcal{K}$ is:

$$|\mathcal{F}_k| = |\Gamma_k| = \frac{D!}{(D - N_k)!}$$

With our specific factorization, an oracle function $f$ can be given as follows:

$$f \in \bigcup_{k \in \mathcal{K}} \mathcal{F}_k \leftrightarrow (k, \gamma) \in \mathcal{K} \times \Gamma_k$$

(3.18)

where $\gamma \in \Gamma_k$ is the unique map such that the diagram in figure 3.1 commutes.

Our first result pertains to the form of the subgroup states $\{ \rho_{k,v} \}_{k \in \mathcal{K}}$.

**Theorem 3.3.2.** Let the subgroup hidden by the oracle be $H_k \in \mathcal{K}$. Let $|v\rangle$ be a slate. Then the subgroup state $\rho_{k,v}$ is given by an element $\varphi_{k,v} \in \mathbb{C}[G]$ acting by the right regular representation:

$$\rho_{k,v} = R(\varphi_{k,v})$$

$$\varphi_{k,v} = |\beta_{v,0}|^2 |\varphi_0\rangle + (1 - |\beta_{v,0}|^2) |\varphi_{k,0}\rangle$$

where $\beta_{v,0} = \langle \omega^0 | v \rangle$ is as defined in (3.10), and:

$$|\varphi_0\rangle = \frac{1}{|G|} \sum_{g \in G} |g\rangle$$

$$|\varphi_{k,0}\rangle = \frac{1}{|G|} \left( \frac{D}{(D - 1)} \sum_{h \in H_k} |h\rangle - \frac{1}{(D - 1)} \sum_{g \in G} |g\rangle \right)$$
Proof. We begin by defining the coset state for $gH_k \in G/H_k$:

$$|gH_k\rangle := \frac{1}{\sqrt{|H_k|}} \sum_{h \in H_k} |gh\rangle$$

For an oracle function $f \in \mathcal{F}_k$, we rewrite the mixed state of the query register (3.11) in terms of the coset states, taking account of the oracle function property that it factors through quotient by $H_k$. Hence, using (3.15) we can write:

$$\rho_{f,v} = \frac{1}{N_k} \sum_{y \in X} |\beta_{v,y}|^2 \sum_{c,c' \in G/H_k} \omega^{-y(\tilde{f}(c)-\tilde{f}(c'))}|c\rangle\langle c'|$$

Under the identifications (3.14) and (3.18): $f \leftrightarrow (k, \gamma)$. We can recast $\rho_{f,v}$ as:

$$\rho_{f,v} = \frac{1}{N_k} \sum_{y \in X} |\beta_{v,y}|^2 \sum_{r,r' \in X_{N_k}} \omega^{-y(\gamma(r)-\gamma(r'))}|\iota_k(r)\rangle\langle \iota_k(r')|$$

Averaging over all $\gamma \in \Gamma_k$ from (3.16), results in the subgroup state $\rho_{k,v}$ (3.12).

$$\rho_{k,v} = \frac{(D - N_k)!}{D!} \sum_{\gamma \in \Gamma_k} \rho_{f,v}$$

$$= \sum_{y \in X} |\beta_{v,y}|^2 \frac{(D - N_k)!}{D!} \sum_{\gamma \in \Gamma_k} \frac{1}{N_k} \sum_{r,r' \in X_{N_k}} \omega^{-y(\gamma(r)-\gamma(r'))}|\iota_k(r)\rangle\langle \iota_k(r')|$$

Since the sets $S_\gamma$ (3.17) all have the cardinality $(D - N_k)!$, we can average over $S_X$ instead of $\Gamma_k$. Then:

$$\rho_{k,v} = \sum_{y \in X} |\beta_{v,y}|^2 \left( \frac{1}{D!} \sum_{\sigma \in S_X} \frac{1}{N_k} \sum_{r,r' \in X_{N_k}} \omega^{-y(\sigma(r)-\sigma(r'))}|\iota_k(r)\rangle\langle \iota_k(r')| \right)$$

For $y \in X$, we define:

$$\hat{\rho}_{k,y} = \frac{1}{D!} \sum_{\sigma \in S_X} \frac{1}{N_k} \sum_{r,r' \in X_{N_k}} \omega^{-y(\sigma(r)-\sigma(r'))}|\iota_k(r)\rangle\langle \iota_k(r')|$$
Then we write $\rho_{k,v}$ as:

$$\rho_{k,v} = \sum_{y \in X} |\beta_{v,y}|^2 \hat{\rho}_{k,y}$$  (3.19)

We consider the operators $\hat{\rho}_{k,y}$ above for $y \in X$. When $y = 0$:

$$\hat{\rho}_{k,0} = \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \right) \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} \langle g| \right)$$  (3.20)

which is simply the projection on the equal superposition state in $\mathbb{C}[G]$.

When $y \neq 0$, we find that:

$$\hat{\rho}_{k,y} = \frac{1}{D^!} \sum_{\sigma \in S_X} \frac{1}{N_k} \left( \sum_{r \in X_{N_k}} |t_k(r)\rangle \langle t_k(r)| + \sum_{r \neq r' \in X_{N_k}} \omega^{-y(\sigma(r)-\sigma(r'))} |t_k(r)\rangle \langle t_k(r')| \right)$$

$$= \frac{1}{N_k} \left( \sum_{r \in X_{N_k}} |t_k(r)\rangle \langle t_k(r)| + \sum_{r \neq r' \in X_{N_k}} |t_k(r)\rangle \langle t_k(r')| \left( \frac{1}{D^!} \sum_{\sigma \in S_X} \omega^{-y(\sigma(r)-\sigma(r'))} \right) \right)$$

The set $\{r \neq r' \in X_{N_k}\}$ can be written as $X_{N_k} \times X_{N_k} \setminus \Delta(X_{N_k})$, where $\Delta$ denotes the diagonal map defined for any set $S$ as:

$$\Delta : S \rightarrow S \times S, \ s \mapsto (s, s)$$

We compute the sum in the inside bracket in the expression for $\hat{\rho}_{k,y}$ above. For a pair $(r, r') \in X_{N_k} \times X_{N_k} \setminus \Delta(X_{N_k})$, define the set $\Omega_{(r,r')}$ of pairs obtained by evaluating permutations in $S_X$ on the pair $(r, r')$.

$$\Omega_{(r,r')} := \{(\sigma(r), \sigma(r')) : \sigma \in S_X\} \subseteq X \times X \setminus \Delta(X)$$

We make two observations. Firstly, $\Omega_{(r,r')} = X \times X \setminus \Delta(X)$. Secondly, for every pair $(s, s') \in X \times X \setminus \Delta(X)$ the set $\{\sigma \in S_X : (\sigma(r), \sigma(r')) = (s, s')\}$ has cardinality
\( (D - 2)! \), and such sets partition \( S_X \). They imply:

\[
\frac{1}{D!} \sum_{\sigma \in S_X} \omega^{-y \cdot \sigma(r) - \sigma(r')} = \frac{(D - 2)!}{D!} \sum_{(s, s') \in \Omega(r, r')} \omega^{-y \cdot (s - s')}
\]

\[
= \frac{(D - 2)!}{D!} \sum_{(s, s') \in X \times X \setminus \Delta(X)} \omega^{-y \cdot (s - s')}
\]

\[
= \frac{(D - 2)!}{D!} \sum_{x \in X \setminus \{0\}} D \omega^{-y \cdot x}
\]

\[
= -\frac{(D - 2)!}{D!} D
\]

\[
= -\frac{1}{(D - 1)}
\]

where the second to last equality is straightforward from the fact that any non-trivial irreducible character of a finite group sums to 0. We continue with \( \tilde{\rho}_{k,y} \) simplification:

\[
\tilde{\rho}_{k,y} = \frac{1}{N_k} \left( \sum_{r \in X_{N_k}} |\iota_k(r) \rangle \langle \iota_k(r) | - \frac{1}{(D - 1)} \sum_{r \neq r' \in X_{N_k}} |\iota_k(r) \rangle \langle \iota_k(r') | \right)
\]

\[
= \frac{1}{N_k} \left( \frac{D}{(D - 1)} \sum_{r \in X_{N_k}} |\iota_k(r) \rangle \langle \iota_k(r) | - \frac{1}{(D - 1)} \sum_{r, r' \in X_{N_k}} |\iota_k(r) \rangle \langle \iota_k(r') | \right)
\]

With the identification in (3.14), this becomes:

\[
\tilde{\rho}_{k,y} = \frac{1}{N_k} \left( \frac{D}{(D - 1)} \sum_{c \in G/H_k} |c \rangle \langle c | - \frac{1}{(D - 1)} \sum_{c, c' \in G/H_k} |c \rangle \langle c' | \right)
\]

It is worth noticing in the above expression that:

\[
\sum_{c \in G/H_k} |c \rangle \langle c |
\]
is the projection on the span of coset states associated with $H_k$, and

$$
\sum_{c,c' \in G/H_k} |c\rangle \langle c'| = N_k \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \right) \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} \langle g| \right) = N_k \tilde{\rho}_{k,0}
$$

where $\tilde{\rho}_{k,0}$ is as in (3.20).

We see that $\tilde{\rho}_{k,y}$ is independent of $y$, and $\tilde{\rho}_{k,0}$ is also independent of $k$. Consequently, we define:

$$
\tilde{\rho}_0 := \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \right) \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} \langle g| \right)
$$

$$
\tilde{\rho}_{k,\bar{0}} := \frac{1}{N_k} \left( \frac{D}{D - 1} \sum_{c \in \text{G/H}_k} |c\rangle \langle c| - \frac{1}{D - 1} \sum_{c,c' \in \text{G/H}_k} |c\rangle \langle c'| \right)
$$

(3.21)

from which follows that we can write $\rho_{k,v}$ in (3.19) as:

$$
\rho_{k,v} = \sum_{y \in X} |\beta_{v,y}|^2 \tilde{\rho}_{k,y}
$$

$$
= |\beta_{v,0}|^2 \tilde{\rho}_0 + (1 - |\beta_{v,0}|^2) \tilde{\rho}_{k,\bar{0}}
$$

One readily checks that the operators $\tilde{\rho}_0$ in (3.20) and $\tilde{\rho}_{k,\bar{0}}$ in (3.21) commute with the left translation (3.6):

$$
L^{-1}(z)\tilde{\rho}_0 L(z) = \tilde{\rho}_0
$$

$$
L^{-1}(z)\tilde{\rho}_{k,\bar{0}} L(z) = \tilde{\rho}_{k,\bar{0}} \quad \forall z \in G
$$

which implies that $\tilde{\rho}_0$ and $\tilde{\rho}_{k,\bar{0}}$ are given by elements of $\mathbb{C}[G]$ acting by the right regular representation, found by evaluating the two operators at the identity of $\mathbb{C}[G]$. We write:

$$
\tilde{\rho}_0 = R(\langle \varphi_0 |)
$$

$$
\tilde{\rho}_{k,\bar{0}} = R(\langle \varphi_{k,\bar{0}} |)
$$
where:

\[ |\varphi_0\rangle = \frac{1}{|G|} \sum_{g \in G} |g\rangle \]

\[ |\varphi_{k,0}\rangle = \frac{1}{|G|} \left( \frac{D}{(D-1)} \sum_{h \in H_k} |h\rangle - \frac{1}{(D-1)} \sum_{g \in G} |g\rangle \right) \]

\[ 3.4 \text{ The character query and optimal measurements} \]

To compare ESTP queries, we would like to quantify a query by the highest success probability it can achieve with any measurement. In that connection, we denote by \( \mathcal{E}_G \) the set of all POVMs on the query register: \( \mathcal{E}_G := \{ \mathcal{E} : \mathcal{E} \text{ a POVM on } \mathbb{C}[G] \} \).

Fix a slate \( |v\rangle \). Given that the oracle hides the subgroup \( H_k \), the probability of correctly identifying it using a measurement \( \mathcal{E} = \{ E_k \}_{k \in \mathcal{K}} \) is \( \mu_{v,\mathcal{E}}(k|k) = \mathrm{tr}(E_k \rho_{k,v}) \) by (3.13). All the subgroups in the set of subgroups \( \mathcal{I} \) are equally likely to be hidden by the oracle, with a uniform prior probability over \( \mathcal{I} \). So the probability of successful subgroup identification denoted \( S_{v,\mathcal{E}} \) is:

\[ S_{v,\mathcal{E}} = \frac{1}{K} \sum_{k \in \mathcal{K}} \mu_{v,\mathcal{E}}(k|k) = \frac{1}{K} \sum_{k \in \mathcal{K}} \mathrm{tr}(E_k \rho_{k,v}) \]

This is exactly the probability of successful state discrimination in (3.4) in which the measurement \( \mathcal{E} = \{ E_k \}_{k \in \mathcal{K}} \) is used to distinguish the subgroup states \( \{ \rho_{k,v} \}_{k \in \mathcal{K}} \) distributed with prior probability \( \{ p_k \}_{k \in \mathcal{K}} \) given by \( p_k = 1/K \) (section 3.1.2). As \( \mathcal{E} \) varies over \( \mathcal{E}_G \), we get a function \( S_v \) on the set of POVMs \( \mathcal{E}_G \), giving the probability of successful subgroup identification.

**Definition 3.4.1.** The success probability of a slate \( |v\rangle \), denoted by \( S_v \), is a function
on $\mathcal{E}_G$:

$$S_v : \mathcal{E}_G \rightarrow [0, 1]$$

$$\mathcal{E} = \{E_k\}_{k \in \mathcal{K}} \mapsto S_{v, \mathcal{E}} = \frac{1}{K} \sum_{k \in \mathcal{K}} \text{tr}(E_k \rho_{k,v})$$

We call $S_v(\mathcal{E})$ the success probability of the slate $|v\rangle$ for the measurement $\mathcal{E}$.

To see the topological structure of $\mathcal{E}_G$, a useful alternate description of a measurement is:

$$\mathcal{E} := (E_k)_{k \in \mathcal{K}} \in \text{End}(\mathbb{C}[G])^\times \mathcal{K}$$

where the $\{E_k\}_{k \in \mathcal{K}}$ satisfy the conditions in section 3.3. $\text{End}(\mathbb{C}[G])$ is a finite dimensional Hilbert space. Give $\text{End}(\mathbb{C}[G])^\times \mathcal{K}$ the product topology. Then $\mathcal{E}_G$ is a compact subset of $\text{End}(\mathbb{C}[G])^\times \mathcal{K}$. Given a slate $|v\rangle$, $S_v$ is continuous. Hence we can define the maximum probability, over $\mathcal{E}_G$, of correctly determining a hidden subgroup with a slate $|v\rangle$.

**Definition 3.4.2.** The *optimum success probability* of a slate $|v\rangle$, denoted by $\hat{S}_v$, is:

$$\hat{S}_v := \max_{\mathcal{E} \in \mathcal{E}_G} \{S_v(\mathcal{E})\}$$

By the definition of $\hat{S}_v$, there is some measurement that achieves it. Such measurements may not be unique.

**Definition 3.4.3.** A measurement $\mathcal{E} \in \mathcal{E}_G$ is an *optimal measurement* for a slate $|v\rangle$ if $S_v(\mathcal{E}) = \hat{S}_v$.

We will also need a basic result from the representation theory of finite groups [26]. Let $\hat{G}$ be the equivalence classes of irreducible unitary representations of $G$. Fix a representation $(\pi^\lambda, V^\lambda)$ in the class $\lambda$ for each $\lambda \in \hat{G}$. Its dual representation is denoted by $(\pi^{\lambda^*}, V^{\lambda^*})$. Let the dimension of $V^\lambda$ be $d_\lambda$. Then the right translation (3.6) is isomorphic to:

$$R(z) \cong \bigoplus_{\lambda \in \hat{G}} I_{V^{\lambda^*}} \otimes \pi^\lambda(z) \quad (3.22)$$
where $I_{V^\lambda}$ is the identity operator on the space $V^\lambda$. We denote the trivial representation by $(\tau^0, V^0)$.

Next, we define some specific queries that will be needed in the computation of success probabilities.

**Definition 3.4.4.** The character query, the standard query, and the constant query, are defined by their slates and the identification $t_{S_0}$ in (3.8).

The _constant query:_ $|\Psi_0\rangle := t_{S_0}|v_0\rangle, \quad |v_0\rangle := |\chi_{(0,0,...,0)}\rangle$

The _standard query:_ $|\Psi_s\rangle := t_{S_0}|v_s\rangle, \quad |v_s\rangle := |(0,0,...,0)\rangle$

The _character query:_ $|\Psi_c\rangle := t_{S_0}|v_c\rangle, \quad |v_c\rangle := |\chi_{(1,0,...,0)}\rangle$

where $|\chi_y\rangle$ is as in (3.9).

We express the success probability of any given ESTP query as a function of that of the character query, and show that the optimal measurements are common to almost all the queries.

**Corollary 3.4.5.** (i) For any measurement $\U = \{U_k\}_{k \in \mathcal{X}}$, there is a measurement $\mathcal{E} = \{E_k\}_{k \in \mathcal{X}}$ of the form:

$$E_k \equiv \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda} \otimes E^\lambda_k, \quad E^\lambda_k \in \text{End}(V^\lambda)$$

hence given by elements of $\mathbb{C}[G]$ acting by the right regular representation, such that $\U$ and $\mathcal{E}$ have the same conditional probabilities in (3.13). That is:

$$\mu_{v,\U}(k'|k) = \mu_{v,\mathcal{E}}(k'|k) \quad \forall |v\rangle \in S_0, \quad k, k' \in \mathcal{X}$$

In particular, $S_v(\U) = S_v(\mathcal{E}) \quad \forall |v\rangle \in S_0$.

(ii) Let $|v\rangle$ be a slate. Given a measurement $\mathcal{E} \in \mathcal{E}_G$, the success probability of
$|v\rangle$ for $\mathcal{E}$, $S_v(\mathcal{E})$, is:

$$S_v(\mathcal{E}) = \frac{|\beta_{v,0}|^2}{K} + (1 - |\beta_{v,0}|^2)S_v(\mathcal{E})$$

In particular, if a measurement is optimal for some slate $|v\rangle$ such that $|\beta_{v,0}| \neq 1$ ($|v\rangle \notin \{e^{i\theta}|v_0\rangle : \theta \in \mathbb{R}\}$), then it is optimal for every slate.

Proof. (i): Suppose we are given a slate $|v\rangle$, and a measurement $\mathcal{U} = \{U_k\}_{k \in K}$.

Then $\mu_{v,\mathcal{U}}(k'|k) = \text{tr}(U_k\rho_{k,v})$.

Each operator $\rho_{k,v}$ is isomorphic to a direct sum by Theorem 3.3.2 and (3.22). Define $\tilde{\rho}_{k,v}$ as:

$$\rho_{k,v} \cong \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda} \otimes \pi^\lambda(\varphi_{k,v}) =: \tilde{\rho}_{k,v} \quad (3.23)$$

We have that: the trace of a linear operator on a finite dimensional vector space is invariant under vector space isomorphisms, $\tilde{\rho}_{k,v}$ is a direct sum, and $\text{End}(V^\lambda) \cong \text{End}(V^\lambda) \otimes \text{End}(V^\lambda)$. Thus, there exists $\tilde{E}_{k'} \in \bigoplus_{\lambda \in \hat{G}} \text{End}(V^\lambda) \otimes \text{End}(V^\lambda)$ such that: $\text{tr}(\tilde{E}_{k'}\tilde{\rho}_{k,v}) = \text{tr}(U_{k'}\rho_{k,v})$. Trace, $\text{tr}: \text{End}(V^\lambda) \otimes \text{End}(V^\lambda) \to \mathbb{C}$, has the property:

$$\text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B) \quad \forall A \in \text{End}(V^\lambda), \ B \in \text{End}(V^\lambda)$$

This, together with the form of the summands $I_{V^\lambda} \otimes \pi^\lambda(\varphi_{k,v})$ in (3.23), implies that $\tilde{E}_{k'}$ can be chosen so that:

$$\tilde{E}_{k'} = \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda} \otimes E_{k'}^\lambda$$

for some $E_{k'}^\lambda \in \text{End}(V^\lambda)$. Under the isomorphism (3.22), we can find $E_{k'}$:

$$E_{k'} \cong \tilde{E}_{k'} = \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda} \otimes E_{k'}^\lambda$$

(ii): Let $\mathcal{E} = \{E_k\}_{k \in \mathcal{K}}$. Using Theorem 3.3.2, we can write $S_v(\mathcal{E})$ as:
\[ S_v(\mathcal{E}) = \frac{1}{K} \sum_{k \in \mathcal{X}} \text{tr}(E_k \rho_{k,v}) \]
\[ = |\beta_{v,0}|^2 \frac{1}{K} \sum_{k \in \mathcal{X}} \text{tr}(E_k \tilde{\rho}_o) + (1 - |\beta_{v,0}|^2) \frac{1}{K} \sum_{k \in \mathcal{X}} \text{tr}(E_k \tilde{\rho}_{k,0}) \] (3.24)

Notice that the definition of \(|v_c\rangle\) makes \(\beta_{0,v_c} = 0\). By Theorem 3.3.2, \(\rho_{k,v_c} = \tilde{\rho}_{k,0} = R(|\varphi_{k,0}\rangle)\), which makes \(S_{v_c}(\mathcal{E})\):
\[ S_{v_c}(\mathcal{E}) = \frac{1}{K} \sum_{k \in \mathcal{X}} \text{tr}(E_k \tilde{\rho}_{k,0}) \] (3.25)

Because \(\sum_{k \in \mathcal{X}} E_k = I\) and \(\text{tr}(\tilde{\rho}_o) = 1\),
\[ \frac{1}{K} \sum_{k \in \mathcal{X}} \text{tr}(E_k \tilde{\rho}_o) = \frac{1}{K} \text{tr}(\tilde{\rho}_o) = \frac{1}{K} \]

This simplifies \(S_v(\mathcal{E})\) in (3.24).
\[ S_v(\mathcal{E}) = \frac{|\beta_{v,0}|^2}{K} + (1 - |\beta_{v,0}|^2) S_{v_c}(\mathcal{E}) \] (3.26)

3.5 Success probability of the character query

We are ready to show that the character query has the maximum success probability, strictly higher than that of the standard query. Once we have shown this, we take a closer look at the Deutsch’s problem for single bit.

Corollary 3.5.1. The optimum success probabilities satisfy:
\[ \frac{1}{K} \leq \hat{S}_v \leq \hat{S}_{v_c} \forall |v\rangle \in S_0 \]

The lower equality is true if and only if \(|\beta_{v,0}| = 1\) \(\{|v\rangle \in \{e^{i\theta}|v_0\rangle : \theta \in \mathbb{R}\}\}\), and the upper equality is true if and only if \(\beta_{v,0} = 0\). In particular, \(\hat{S}_{v_s} < \hat{S}_{v_c}\).
**Proof.** First, define the trivial measurement to be $\mathcal{T} = \{T_k\}$, $T_k = \frac{1}{K} I$, where $I$ is the identity operator on $\mathbb{C}[G]$. The success probability of the trivial measurement, for any slate $|v\rangle$, is $S_v(\mathcal{T}) = \frac{1}{K}$. This is because $\text{tr}(\rho_{k,v}) = 1 \ \forall k \in \mathcal{K}$.

By Corollary 3.4.5 (ii), we just need to show that there exists a measurement $M \in \mathcal{E}_G$ which has a success probability of the character query for $M$, $S_v(\mathcal{M})$, greater than $\frac{1}{K}$. Since the trivial measurement $\mathcal{T}$ has success probability $\frac{1}{K}$, it is sufficient to show:

$$\exists \mathcal{M} \in \mathcal{E}_G : S_v(\mathcal{M}) > S_v(\mathcal{M})$$

(3.27)

Before defining $\mathcal{M}$, we consider the subgroup states for the character query, $\{\rho_{k,v_c}\}_{k \in \mathcal{K}}$. As seen in Corollary 3.4.5, $\rho_{k,v_c} = R(|\varphi_{k,0}\rangle)$. Decompose each $|\varphi_{k,0}\rangle$ into its Fourier components, denoted by $\tilde{\varphi}_k^\lambda$ for $\lambda \in \hat{G}$.

$$\tilde{\varphi}_k^0 := \pi^0(|\varphi_{k,0}\rangle)$$

$$= \frac{1}{|G|} \left( \frac{D}{(D-1)} \sum_{h \in H_k} \pi^0(h) - \frac{1}{(D-1)} \sum_{g \in G} \pi^0(g) \right)$$

$$= \frac{D}{(D-1)|H_k|} - \frac{1}{(D-1)|G|}$$

$$= \frac{D - N_k}{(D-1)N_k}$$

(3.28)

For every non-trivial representation $\lambda \in \hat{G} \setminus \{0\}$:

$$\tilde{\varphi}_k^\lambda := \pi^\lambda(|\varphi_{k,0}\rangle)$$

$$= \frac{1}{|G|} \frac{D}{(D-1)} \sum_{h \in H_k} \pi^\lambda(h)$$

$$= \frac{D}{(D-1)N_k} \frac{1}{|H_k|} \sum_{h \in H_k} \pi^\lambda(h)$$

(3.29)

Also define:

$$\tilde{\varphi}^\lambda := \frac{1}{K} \sum_{k \in \mathcal{K}} \tilde{\varphi}_k^\lambda$$
Note that:
\[
\text{Ker}(\tilde{\varphi}^\lambda) = \bigcap_{k \in \mathcal{X}} \text{Ker}(\tilde{\varphi}_k^\lambda)
\]
\[
\text{Im}(\tilde{\varphi}^\lambda) = V^\lambda \setminus \text{Ker}(\tilde{\varphi}^\lambda)
\]

We take the measurement \( \mathcal{M} = \{M_k\} \) to be the Pretty Good Measurement from section 3.1.2 (3.5), for the subgroup states \( \{\rho_{k,vc}\}_{k \in \mathcal{X}} \) with prior probability \( \{p_k\}_{k \in \mathcal{X}} \) given by \( p_k = 1/K \). Using (3.23) and the definitions above we can write the subgroup states as:
\[
\rho_{k,vc} \approx \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda^*} \otimes \tilde{\varphi}_k^\lambda
\]
and compute the PGM:
\[
M_k \approx \bigoplus_{\lambda \in \hat{G}} I_{V^\lambda^*} \otimes M_k^\lambda
\]
where:
\[
M_k^\lambda = \frac{1}{K} \left( (\tilde{\varphi}^\lambda)^{-1/2} \tilde{\varphi}_k^\lambda (\tilde{\varphi}^\lambda)^{-1/2} \oplus I_{\text{Ker}(\tilde{\varphi}^\lambda)} \right)
\]
Here \( I_{\text{Ker}(\tilde{\varphi}^\lambda)} \) is the identity operator on \( \text{Ker}(\tilde{\varphi}^\lambda) \), and \( (\tilde{\varphi}^\lambda)^{-1/2} \) is:
\[
(\tilde{\varphi}^\lambda)^{-1/2} := (\tilde{\varphi}^\lambda |_{\text{Im}(\tilde{\varphi}^\lambda)})^{-1/2} \oplus I_{\text{Ker}(\tilde{\varphi}^\lambda)}
\]

From (3.25), the success probabilities of the character query for the PGM \( \mathcal{M} \) and the trivial measurement \( \mathcal{T} \) are:
\[
S_{vc}(\mathcal{M}) = \frac{1}{K} \sum_{\lambda \in \hat{G}} d_\lambda \sum_{k \in \mathcal{X}} \text{tr} \left( M_k^\lambda \tilde{\varphi}_k^\lambda \right) = \frac{1}{K} \sum_{\lambda \in \hat{G}} d_\lambda \sum_{k \in \mathcal{X}} \frac{1}{K} \text{tr} \left( (\tilde{\varphi}^\lambda)^{-1/2} \tilde{\varphi}_k^\lambda (\tilde{\varphi}^\lambda)^{-1/2} \oplus I_{\text{Ker}(\tilde{\varphi}^\lambda)} \right)
\]
\[
S_{vc}(\mathcal{T}) = \frac{1}{K} \sum_{\lambda \in \hat{G}} d_\lambda \sum_{k \in \mathcal{X}} \text{tr} \left( T_k^\lambda \tilde{\varphi}_k^\lambda \right) = \frac{1}{K} \sum_{\lambda \in \hat{G}} d_\lambda \text{tr} \left( \tilde{\varphi}^\lambda \right)
\]

We recall the inner product and norm on \( M_{d_\lambda}(\mathbb{C}) \):
\[
< A, B > = \text{tr} \left( AB^\dagger \right)
\]
\[
\|A\| = \sqrt{\text{tr} \left( AA^\dagger \right)}
\]
where $A, B \in M_d^\lambda(C)$. This allows $S_{vc}(\mathcal{M})$ and $S_{vc}(\mathcal{T})$ to be expressed as:

$$S_{vc}(\mathcal{M}) = \frac{1}{K} \sum_{\lambda \in \hat{G}} d_\lambda \sum_{k \in \mathbb{K}} \frac{1}{K} \| (\tilde{\phi}^\lambda)^{-1/4} \tilde{\phi}_k^\lambda (\tilde{\phi}^\lambda)^{-1/4} \|^2$$

$$S_{vc}(\mathcal{T}) = \frac{1}{K} \sum_{\lambda \in \hat{G}} d_\lambda \| (\tilde{\phi}^\lambda)^{1/2} \|^2$$

Then the inequality in (3.27) follows from these additional observations:

(i) $\exists \lambda \in \hat{G}$, and $k, k' \in \mathbb{K}$ such that $\tilde{\phi}_k^\lambda \neq \tilde{\phi}_k^{\lambda'}$

(ii) $\sum_{k \in \mathbb{K}} (\tilde{\phi}^\lambda)^{-1/4} \tilde{\phi}_k^\lambda (\tilde{\phi}^\lambda)^{-1/4} = K (\tilde{\phi}^\lambda)^{1/2} \quad \forall \lambda \in \hat{G}$

and the next lemma.

**Lemma 3.5.2.** Let $V$ be a finite dimensional Hilbert space over $C$. Let $\{v_i\}_{i=1}^n$ be a set of vectors in $V$. Then:

$$\frac{1}{n} \| \sum_{i=1}^n v_i \|^2 \leq \sum_{i=1}^n \| v_i \|^2$$

with equality if and only if $v_i = v_j \forall i, j \in \{1, \ldots, n\}$.

Proof.

$$n \sum_{i=1}^n \| v_i \|^2 - \sum_{i=1}^n \| v_i \|^2 = n \sum_{i=1}^n \| v_i \|^2 - \sum_{i,j=1}^n \langle v_i, v_j \rangle$$

$$= (n - 1) \sum_{i=1}^n \| v_i \|^2 - \sum_{1 \leq i < j \leq n} (\langle v_i, v_j \rangle + \langle v_j, v_i \rangle)$$

$$\geq (n - 1) \sum_{i=1}^n \| v_i \|^2 - \sum_{1 \leq i < j \leq n} 2\| v_i \| \| v_j \|$$

$$= \sum_{1 \leq i < j \leq n} (\| v_i \|^2 - 2\| v_i \| \| v_j \| + \| v_j \|^2$$

$$= \sum_{1 \leq i < j \leq n} (\| v_i \| - \| v_j \|)^2$$

where the inequality above is a result of the Cauchy-Schwarz inequality. The lemma follows. \qed
Remark 3.5.3. In view of Corollary 3.4.5, an optimal measurement \( \hat{E} = \{ \hat{E}_k \} \) can be described by:
\[
\hat{E}_k \cong \bigoplus_{\lambda \in \hat{G}} I_{V^{\lambda*}} \otimes \hat{E}_k^\lambda
\]
Using (3.28) and (3.29):
\[
\hat{S}_{vc} = \frac{1}{K} \sum_{k \in \mathcal{X}} \left[ \frac{D - N_k}{(D - 1)N_k} + \frac{D}{(D - 1)|G|} \sum_{\lambda \in \hat{G} \setminus \{0\}} d_{\lambda} \sum_{h \in H_k} \text{tr}(\hat{E}_k^\lambda \pi^\lambda(h)) \right]
\]
(3.30)
Therefore, the character query performs better as the dimension \( D \) of the response register decreases.

Remark 3.5.4. From the definition of the standard query, \( \beta_{0,v_s} = 1/\sqrt{D} \). We conclude from Corollary 3.4.5 (ii) that \( \lim_{D \to \infty} \hat{S}_{vc} = \hat{S}_{vs} \). So the optimum success probability of the character query decreases to that of the standard query as the dimension of the response register increases.

We now turn our attention to the Deutsch’s problem for single bit \( (n = 1) \) and understand it in our framework. Let us restate the set up from section 3.1.2. The group \( G = \mathbb{Z}_2 \). The response space is \( X = \mathbb{Z}_2 \). Possible hidden subgroups are: \( H_0 := G \) and \( H_1 := \{0\} \). Constant functions hide the subgroup \( H_0 \) and balanced functions hide \( H_1 \). The subgroup indices are \( N_0 = 1 \) and \( N_1 = 2 \) respectively. The system on which the oracle and measurement act is:
\[
\mathcal{H} := \mathbb{C}[G] \otimes \mathbb{C}[X] = \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_2]
\]
where the first tensor factor \( \mathbb{C}[G] \) is the query register, and the second factor \( \mathbb{C}[X] \) is the response register. Since \( X = \mathbb{Z}_2 \), this makes the dimension of the response register \( D = 2 \). The group \( G = \mathbb{Z}_2 \) has two 1-dimensional representations: the trivial representation and the alternating representation.
\[
\begin{align*}
\pi^0(x) &= 1 \\
\pi^{-}(x) &= (-1)^x
\end{align*}
\]
\( \forall x \in \mathbb{Z}_2 \)
Phase kickback harnesses the character query: \( |\Psi_c\rangle = |+\rangle |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\chi_1\rangle \),
where \( \omega = -1 \), and \( |v_c\rangle = |\chi_1\rangle = |\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \). After the oracle evaluation, we can use (3.28) and (3.29) to deduce the Fourier components of the subgroup states \( \rho_{k,v_c} = R(|\varphi_{k,\bar{a}}\rangle) \).

\[
\rho_{0,v_c} \cong \pi^0(|\varphi_{0,\bar{a}}\rangle) \oplus \pi^-(|\varphi_{0,\bar{a}}\rangle) = 1 \oplus 0 \\
\rho_{1,v_c} \cong \pi^0(|\varphi_{1,\bar{a}}\rangle) \oplus \pi^-|\varphi_{1,\bar{a}}\rangle) = 0 \oplus 1
\]

We choose a measurement \( \mathcal{E} := \{E_k\}_{k \in \{0,1\}} \) as follows:

\[
E_k \cong E_k^0 \oplus E_k^-
\]

where:

\[
E_0 \cong E_0^0 \oplus E_0^- = 1 \oplus 0 \\
E_1 \cong E_1^0 \oplus E_1^- = 0 \oplus 1
\]

By (3.25), this measurement has a probability of success \( S_{v_c}(\mathcal{E}) = 1 \). This is precisely what we call the measurement for Deutsch’s problem in section 3.1.1. By using the Hadamard transform \( H \), the character basis of \( \mathbb{C}[\mathbb{Z}_2] \) is rotated to the computational basis, i.e.:

\[
H : \begin{cases} \\
\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \mapsto |0\rangle \\
\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \mapsto |1\rangle
\end{cases}
\]

Measuring in the computational basis is then equivalent to the measurement above. It is because the subgroup \( H_1 = \{0\} \) has an index the same as the dimension of the response register, \( N_1 = D \), that it has no projection on the trivial representation. In contrast, the subgroup \( H_0 = G \) has an index less than the dimension of the response register, \( N_0 < D \), which results in its producing a non-zero projection on the trivial representation. That is why the subgroups can be distinguished with probability 1. This illustrates the part played by the dimension of the response
register relative to the subgroup indices, and explains the algorithm in the group representation context.

3.6 Conjugate subgroups

We specialize further to a class of subgroups consisting of conjugates of a particular subgroup \( H \leq G \), i.e., \( \mathcal{S} = \{g^{-1}Hg : g \in G\} \), and determine the optimum success probability for any \(|v⟩ \in S_0\). To that end, we exploit a result of Moore and Russell [20]. Plancherel measure, denoted by \( \mu_p \), is the probability distribution on \( \hat{G} \) defined as:

\[
\mu_p(\lambda) := \frac{d^2_\lambda}{|G|} \quad \text{for} \quad \lambda \in \hat{G}
\]

In particular:

\[
\mu_p(0) = \frac{1}{|G|}
\]

As in Moore and Russell [20], define the set \( \Lambda_H \subseteq \hat{G} \):

\[
\Lambda_H := \{ \lambda \in \hat{G} : \frac{1}{|H|} \sum_{h \in H} \pi^\lambda(h) \neq 0 \}
\]

We recognize \( \frac{1}{|H|} \sum_{h \in H} \pi^\lambda(h) \) as the projection onto the space of \( H \)-invariants in \( \lambda \in \hat{G} \).

Denote the normalizer of \( H \) in \( G \) by \( N_G(H) \).

**Corollary 3.6.1.** Let \( H \leq G \), and \( \mathcal{S} = \{gHg^{-1} : g \in G\} \). Let \( N := [G : H] \) and \( N_C := [G : N_G(H)] \). Then for any slate \(|v⟩\), the optimum success probability, \( \hat{S}_v \), is given by:

\[
\hat{S}_v = \left( |\beta_{v,0}|^2 - (1 - |\beta_{v,0}|^2) \frac{1}{(D-1)} \right) \frac{1}{N_C} + (1 - |\beta_{v,0}|^2) \frac{D}{(D-1)} \frac{|H|}{N_C} \mu_p(\Lambda_H)
\]

**Proof.** Let the subgroup indexing set be \( \mathcal{X} = G/N_G(H) \). Then \( K = |\mathcal{X}| = N_C \). As \( \beta_{v,0} = 1/\sqrt{D} \) (the case of standard query), by Corollary 3.4.5 (ii) an optimal measurement for \(|v_s⟩\) is optimal for any slate \(|v⟩\). Moore and Russell [20] have shown that the Pretty Good Measurement (PGM) for the standard query is such
a measurement, and also derived its success probability. Using their result:

$$\hat{S}_{vs} = \frac{|H|}{N_C} \mu_p(\Lambda_H)$$

From Corollary 3.4.5 (ii):

$$\hat{S}_{vs} = \frac{|\beta_{0,vs}|^2}{N_C} + (1 - |\beta_{0,vs}|^2)\hat{S}_{vc}$$

$$= \frac{1}{DN_C} + \frac{(D-1)}{D} \hat{S}_{vc}$$

Together they imply:

$$\hat{S}_{vc} = \frac{D}{(D-1)} \frac{|H|}{N_C} \mu_p(\Lambda_H) - \frac{1}{(D-1)N_C}$$

Applying Corollary 3.4.5 (ii) again, we get the result we seek.

**Remark 3.6.2.** Unlike in Deutsch’s problem, here the subgroup states for the character query all have the same projection on the trivial representation, by (3.28). These contribute nothing toward distinguishing the subgroups, and are eliminated if the dimension of the response register is the same as the index of $H$, i.e., if $D = N$. Assuming such is the case, from the proof of Corollary 3.6.1, the character query succeeds with probability:

$$\hat{S}_{vc} = \frac{N}{(N-1)} \frac{|H|}{N_C} \mu_p(\Lambda_H \setminus \{0\})$$

### 3.7 Conclusion and discussion

We have addressed the problem of query selection for the single-query hidden subgroup problem (HSP) over a general finite group $G$ and an abelian response space $X$. Our results indicate that for a single-query algorithm with measurements of the query register, and among the class of queries in an equal superposition state over the group, we can maximize the subgroup identification (success) probability using a query that has no projection on the constant query (defined as the equal
superposition over the group as well as the response space). The character query is an example of this set of queries contained in the $|X| - 1$ (in the above discussion $D = |X|$) dimensional subspace orthogonal to the constant query.

This generalization of the phase kickback trick explains the phase kickback for Deutsch’s problem (single bit) in representation theoretic terms. It arises naturally when we analyze how the success probability of the algorithm depends on the choice of the query. Imposing some structure (an abelian structure in this discussion) on $X$ is necessary to analyze the effect of different queries. The result that the optimal measurements for algorithms in our class are common to all ESTP queries other than the phase multiples of the constant query, is not something one would expect a priori. It shows why in Deutsch’s problem the phase kickback trick and the standard method have the same optimal measurement. The character query outperforms the query used in the standard method single-query HSP algorithms, and gives an improvement over the success probability of Moore and Russell [20] for conjugate subgroups.

For the character query itself, the success probability decreases as the response register dimension $|X|$ increases; an example is the conjugate subgroups case (where the highest success probability is achieved when the subgroups have the same index as the response register dimension). The response register dimension relative to the subgroup indices differentiates the subgroups through their projection on the trivial representation. This has the potential to improve the success probability, as we saw in the analysis of phase kickback in Deutsch’s problem, which is somewhat more complicated than the conjugate subgroups case.

Our approach towards optimizing single queries for HSP depends on conceptualizing the oracle functions as given by permutations. By computing with the response space $X$, and developing and interpreting results with respect to the group representation one gains insight about queries and oracle action. Finally, recognizing that the structure of the problem allows the use of representation theory in conjunction with the PGM (in general a sub-optimal measurement), and the analysis of measurements using norms, leads to the proof of optimality of the character query.
We expect aspects of this approach, in particular the resulting generalized phase kickback, to have applications in other domains, among them multi-query settings as in Bacon, Childs and Van Dam [21] and Meyer and Pommersheim [24].

Chapter 3, in part, has been submitted for publication of the material as *An improved query for the Hidden Subgroup Problem*, by A. Shakeel. The dissertation author was the primary investigator and author of this paper.
Chapter 4

Some ideas in multi-query optimization

4.1 Introduction

We would like to extend the methods of query selection from the previous chapter to multi-query settings. Parallel queries have been employed before in the context of standard method for dihedral group HSP algorithm [20,21]. We expect to increase the probability of success if not decrease the query complexity by optimization of queries. This is still in the early stages of development. There are some preliminary ideas, some intermediate observations and numerical results that point to the potential of this approach.

Note: For this chapter we call any query of the form \( \frac{1}{\sqrt{|G|}}(\sum_{g \in G} |g\rangle) \otimes |\chi_y\rangle \) (where \( |\chi_y\rangle \) is as in (3.9)) a character query.

4.2 Some analysis of multiple unentangled (pure tensor) queries in parallel

We use the notation from single-query optimization (Chapter 3). As we are using the subscript \( k \) to enumerate the subgroups, we assume we have \( d \) parallel queries (a pure tensor).
The system consists of \( d \) copies of \( \mathbb{C}[G] \otimes \mathbb{C}[X] \):

\[
\mathcal{H}^d = \bigotimes^d \mathbb{C}[G] \otimes \mathbb{C}[X]
\]

where a query:

\[
|\Psi^d\rangle \in \mathcal{H}^d
\]

such that \( \|\Psi^d\| = 1 \).

Then the state after the oracle evaluation is:

\[
\left( \bigotimes^d O_f \right) |\Psi^d\rangle
\]

Denote the mixed state conditioned on the oracle function hiding the subgroup \( H_k \) by \( \rho^d_{f, \Psi^d} \).

\[
\rho^d_{f, \Psi^d} = \bigotimes^d \mathrm{tr}_{c[X]} \left( \bigotimes^d O_f |\Psi^d\rangle \langle \Psi^d| \bigotimes^d O^\dagger_f \right)
\]

As in single-query, every \( f \) arises from some permutation \( \sigma \in S_X \) of \( X \). So we replace \( f \) with \((k, \sigma)\) in the rest of the chapter. We make the identification:

\[
\rho^d_{f, \Psi^d} \leftrightarrow \rho^d_{k, \sigma, \Psi^d}
\]

When considering a parallel query which comprises unentangled (pure tensor of) ESTP queries, we specialize the notation somewhat. We describe the initial state on which the oracles act as:

\[
|\Psi^d\rangle = \bigotimes^d_{i=1} |\Psi_i\rangle
\]

where \( |\Psi_i\rangle = \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle \right) \otimes |v_i\rangle \), and \( |v_i\rangle \in \mathbb{C}[X] \), \( \|v_i\| = 1 \).

Then the state after the oracle evaluation is:

\[
\left( \bigotimes^d O_f \right) |\Psi^d\rangle = \bigotimes^d_{i=1} O_f |\Psi_i\rangle
\]
Define a $k$-tuple of elements of $\mathbb{C}[X]$:

$$\vec{v} := (v_m) = (v_1, \cdots, v_k) \in \mathbb{C}[X]^d$$

Denote the mixed state conditioned on the oracle function hiding the subgroup $H_k$ by $\rho^d_{f,\vec{v}}$.

$$\rho^d_{f,\vec{v}} = \bigotimes^d_{i=1} \text{tr}_{\mathbb{C}[X]} \left( \bigotimes^d_{i=1} \left( O_f |\Psi_i\rangle \langle \Psi_i| O_f^\dagger \right) \right)$$

$$= \bigotimes^d_{i=1} \text{tr}_{\mathbb{C}[X]} \left( O_f |\Psi_i\rangle \langle \Psi_i| O_f^\dagger \right)$$

$$= \bigotimes^d_{i=1} \rho_{f,v_i}$$

where $\rho_{f,v_i}$ is as in (3.11):

$$\rho_{f,v_i} := \text{tr}_{\mathbb{C}[X]} \left( O_f |\Psi_i\rangle \langle \Psi_i| O_f^\dagger \right)$$

$$= \frac{1}{|G|} \sum_{y_i \in X} |\beta_{v_i,y_i}|^2 \left( \sum_{g \in G} \omega^{-y_i \cdot f(g)} |g\rangle \right) \left( \sum_{g' \in G} \omega^{-y_i \cdot f(g')} \langle g'| \right)$$

In terms of the coset states:

$$|gH_k\rangle := \frac{1}{\sqrt{|H_k|}} \sum_{h \in H_k} |gh\rangle$$

and under the identifications (3.14) and (3.18):

$$\rho_{f,v_i} = \frac{1}{N_k} \sum_{y_i \in X} |\beta_{v_i,y_i}|^2 \left( \sum_{r_i \in X_{N_k}} \omega^{-y_i \cdot \gamma(r_i)} \langle \iota_k(r_i) | \right) \left( \sum_{r'_i \in X_{N_k}} \omega^{y_i \cdot \gamma(r'_i)} \langle \iota_k(r'_i) | \right)$$

(4.1)

where $\beta_{v_i,y_i}$, $X_{N_k}$, $\gamma$, and $\iota_k$ are as in Chapter 3.

We make the identifications:

$$\rho^d_{f,v_i} \leftrightarrow \rho^d_{k,\sigma,v_i}$$

$$\rho^d_{f,\vec{v}} \leftrightarrow \rho^d_{k,\sigma,\vec{v}}$$
Define a \( k \)-tuple of elements of the \( X \):

\[
\vec{y} := (y_m) = (y_1, \cdots, y_k) \in X^d
\]

and the rank 1 operator:

\[
\hat{\rho}^d_{k, \sigma, \vec{y}} := \bigotimes_{i=1}^d \frac{1}{N_k} \left( \sum_{r_i \in X_{N_k}} \omega^{-y_i \cdot \sigma(r_i)} |t_k(r_i)\rangle \langle t_k(r_i)| \right) \left( \sum_{r'_i \in X_{N_k}} \omega^{y_i \cdot \sigma(r'_i)} |t_k(r'_i)\rangle \langle t_k(r'_i)| \right) \quad (4.2)
\]

which allows us to write:

\[
\rho^d_{k, \sigma, \vec{v}} = \sum_{\vec{y} \in X^d} \prod_{j=1}^d |\beta_{v_j,y_j}|^2 \hat{\rho}^d_{k, \sigma, \vec{y}}
\]

Averaging over all \( \sigma \in S_X \) results in the subgroup state \( \rho^d_{k, \vec{v}} \):

\[
\rho^d_{k, \vec{v}} = \frac{1}{D!} \sum_{\sigma \in S_X} \rho^d_{k, \sigma, \vec{v}} = \sum_{\vec{y} \in X^d} \prod_{j=1}^d |\beta_{v_j,y_j}|^2 \left( \frac{1}{D!} \sum_{\sigma \in S_X} \hat{\rho}^d_{k, \sigma, \vec{y}} \right) \quad (4.3)
\]

Recall the left and right translation by \( g_0 \in G^\times d \) on \( \vartheta \in \mathbb{C}[G^\times d] \):

\[
L^{\times d}(g_0) \vartheta(g) = \vartheta(g_0^{-1}g) \\
R^{\times d}(g_0) \vartheta(g) = \vartheta(gg_0)
\]

\( \hat{\rho}^d_{k, \sigma, \vec{y}} \) (4.2) in general does not commute with \( L^{\times d} \) action. For \( (g_i) \in G^{\times d} \):

\[
\hat{\rho}^d_{k, \sigma, \vec{y}} \neq L^{\times d}((g_i)) \hat{\rho}^d_{k, \sigma, \vec{y}} L^{\times d}((g_i))^{-1}
\]

unless \( (g_i) = (g, g, \cdots, g) \). This implies \( \rho^d_{k, \vec{v}} \) commutes with the left diagonal translation by \( G \) given by:

\[
L^{\otimes d} := L \otimes L \otimes \cdots \otimes L \quad d \text{ times}
\]
In other words, $\rho_{d,k,\vec{v}}$ is in the commutant of the left diagonal action. In general, finding the commutant of the diagonal action is a hard problem. This is because the irreducible spaces for right $G^{\times d}$ action are reducible under the diagonal action, so the multiplicity spaces for every $\lambda \in \hat{G}$ arise from the decomposition of the irreducible $G^{\times d}$ representations, which are the $d$-fold outer tensor products (see Chapter 1) of the irreducible representations of $G$.

In general this approach does not identify $\rho_{d,k,\vec{v}}$ as an element of the algebra $\mathbb{C}[G^{\times d} \times G^{\times d}]$ acting by left and right translation representations. Thus the state is more complicated, and the representation of the specific group and hidden subgroups under consideration will determine the form of the state $\rho_{d,k,\vec{v}}$. One needs to look for alternate properties of $\rho_{d,k,\vec{v}}$ which might be useful in computations.

There is another aspect to the above assumption on queries. In the expression of $\rho_{d,k,\vec{y},\vec{v}}$ (4.2), each term of the form:

$$
\sum_{r_i \in X_{N_k}} \omega^{-y_i \cdot \sigma(r_i)} |t_k(r_i)\rangle
$$

is an invariant of $H_k$ relative the right regular representation of $G$, that is:

$$
\sum_{r_i \in X_{N_k}} \omega^{-y_i \cdot \sigma(r_i)} |t_k(r_i)\rangle * |H_k\rangle = \sum_{r_i \in X_{N_k}} \omega^{-y_i \cdot \sigma(r_i)} |t_k(r_i)\rangle
$$

Let the projection onto the space of $H_k$-invariants relative the right regular representation of $\mathbb{C}[G]$ be:

$$
P_k = \frac{1}{|H_k|} \sum_{h \in H_k} R(h) \quad (4.4)
$$

This implies every rank 1 operator $\tilde{\rho}_{d,k,\vec{y},\vec{v}}$ (4.2) is a projection into the space of $H_k^{\times d}$ invariants relative the right regular representation $R^{\times d}$ of $G^{\times d}$, i.e. the subspace on which:

$$
\bigotimes_{i=1}^{d} P_k
$$

projects.
4.3 Numerical results and inferences

4.3.1 Improvement through unentangled parallel queries (pure tensor)

We give an example in which extending the character query to the setting of two parallel queries improves the probability of success over the standard method. We consider the dihedral group of order $2N$ with the set of order two subgroups generated by reflections as hidden subgroups (as in Chapter 2). These results are numerical.

For this example, the number of parallel queries, $d = 2$. The response space $X = \mathbb{Z}_N$. We interchange the use permutation notation $\sigma$ with $f$ for oracle functions as suits the description. In each factor, we use a character query given by the corresponding $y_i$ of the previous section. The query is then:

$$|\Psi^2\rangle = \frac{1}{|G|} \left( \sum_{g_1, g_2 \in G} |g_1\rangle|g_2\rangle \right) |\chi_{y_1}\rangle|\chi_{y_2}\rangle$$

(4.5)

and the queried state:

$$\left( \bigotimes^2 \text{O}_f \right) |\Psi^2\rangle = \frac{1}{N} \left( \sum_{r_1, r_2 \in \mathbb{Z}_N} \omega^{-y_1 \cdot \sigma(r_1) - y_2 \cdot \sigma(r_2)} |t_k(r_1)\rangle|t_k(r_2)\rangle \right) |\chi_{y_1}\rangle|\chi_{y_2}\rangle$$

(4.6)

which leads to the mixed states:

$$\tilde{\rho}_{k,\sigma,(y_1,y_2)}^2 = \bigotimes_{i=1}^2 \frac{1}{N} \left( \sum_{r_i \in \mathbb{Z}_N} \omega^{-y_i \cdot \sigma(r_i)} |t_k(r_i)\rangle \right) \left( \sum_{r'_i \in \mathbb{Z}_N} \omega^{y_i \cdot \sigma(r'_i)} \langle t_k(r'_i)| \right)$$

and the subgroup state:

$$\rho_{k,(y_1,y_2)}^2 = \frac{1}{N!} \sum_{\sigma \in S_N} \tilde{\rho}_{k,\sigma,(y_1,y_2)}$$

(4.7)

For comparison, we include the results of the standard query. We use the PGM (Pretty Good Measurement, see Chapters 2, 3) in all the cases. In the table $(s,s)$ signifies that both the queries are standard queries. The pair $(y_1, y_2)$ in other
columns correspond to the particular character queries used.

Table 4.1: Unentangled character queries. Column label: \((y_1, y_2)\)

<table>
<thead>
<tr>
<th></th>
<th>((s, s))</th>
<th>((1, 1))</th>
<th>((1, 2))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(N = 3)</td>
<td>0.765(^1)</td>
<td>0.971(^4)</td>
<td>0.971(^3)</td>
</tr>
<tr>
<td>(N = 4)</td>
<td>0.667(^2)</td>
<td>0.858(^4)</td>
<td>0.955(^5)</td>
</tr>
</tbody>
</table>

\(^1\) \(\frac{5}{9} + \frac{4\sqrt{2}}{27}\), \(^2\) \(\frac{37 + 4\sqrt{2}}{64}\), \(^3\) \((3 + 2\sqrt{2})/6\).
\(^4\) \((291 + 20\sqrt{6} + 8\sqrt{10} + 12\sqrt{15})/480\), \(^5\) \((43 + 2\sqrt{2})/48\).

We see a significant improvement over the standard method by using character queries in parallel. Indeed the success probability is different for different character queries. This confirms that query selection has promise in a multi-query approach and that it is worth extending the character query analysis to parallel queries.

Besides using unentangled parallel queries (pure tensors), other potential avenues for such an improvement are in the use of parallel queries which are not pure tensors, i.e., are entangled.

### 4.3.2 Improvement through entangled parallel queries

Instead of using pure tensors, we can use a more general query. Before that we make some observations. A basis element in our space of interest is given by \(|g\rangle|g\rangle|\chi_{y_1}\rangle|\chi_{y_2}\rangle\).

Before that we make some observations. A basis element in our space of interest is given by \(|g_1\rangle|g_2\rangle|\chi_{y_1}\rangle|\chi_{y_2}\rangle\) (where \(g_1, g_2 \in G\)). In the previous example, consider the queried state \((\bigotimes^2{O}_f)|g_1\rangle|g_2\rangle|\chi_{y_1}\rangle|\chi_{y_2}\rangle\) in the following cases.

Let the characters in the two tensor factors be given by: \((y_1, y_2) = (1, 2)\). When \(g_1 = g_2\) (or the same group element in the two tensor factors), the phase from diagonal elements\(-y_1 \cdot \sigma(g_1) - y_2 \cdot \sigma(g_1) = 0\). So the diagonal elements carry no information about the oracle function. Similarly, let \((y_1, y_2) = (1, 1)\). When \(g_1 = g_2\), the phase \(-y_1 \cdot \sigma(g_1) - y_2 \cdot \sigma(g_2) = -2y_1 \cdot \sigma(g_1)\). This is the same as using just one character query.
Let us define the off-diagonal character query:

$$|\Psi_{OD}\rangle := \frac{1}{\sqrt{|G|^2 - |G|}} \left( \sum_{g_1 \neq g_2 \in G} |g_1\rangle |g_2\rangle \right) |\chi_{y_1}\rangle |\chi_{y_2}\rangle$$

and the diagonal character query:

$$|\Psi_D\rangle := \frac{1}{\sqrt{|G|}} \left( \sum_{g \in G} |g\rangle |g\rangle \right) |\chi_{y_1}\rangle |\chi_{y_2}\rangle$$

Then let the linear combination character query be parameterized by $0 \leq t \leq 1$:

$$|\Psi(t)\rangle := \sqrt{1 - t}|\Psi_{OD}\rangle + \sqrt{t}|\Psi_D\rangle$$

(4.8)

Denote the mixed state conditioned on the oracle function hiding the subgroup $H_k$ by $\rho(t)_{\sigma,(y_1,y_2)}$.

$$\rho(t)_{\sigma,(y_1,y_2)} = \bigotimes_{i=1}^2 \text{tr}_{C[X]} \left( \bigotimes_{j}^2 O_j |\Psi(t)\rangle \langle \Psi(t)| \bigotimes_{j}^2 O_j^\dagger \right)$$

Then, using the PGM as measurement, we list the probabilities of success using the triple $(y_1, y_2, t^\ast)$ (where $t^\ast$ is the optimal value of $t$) to label the columns. We observe that the success probability is 1 in the case $(y_1, y_2, t^\ast) = (1, 1, 4/9)$. This is not achievable by the standard method, an entangled query giving a superior performance than an unentangled one.

Table 4.2: Entangled character queries. Column label: $(y_1, y_2, t^\ast)$

<table>
<thead>
<tr>
<th>Column</th>
<th>$(1, 1, 0)$</th>
<th>$(1, 1, 4/9)$</th>
<th>$(1, 2, 0)$</th>
<th>$(1, 2, 0.05)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N=3$</td>
<td>0.929$^6$</td>
<td>1</td>
<td>0.979$^7$</td>
<td>0.984</td>
</tr>
</tbody>
</table>

$^6$ $(7 + 4\sqrt{3})/15$. $^7$ $(8 + 3\sqrt{2} + \sqrt{6})/15$.

Next, we give the result of using a sequential paradigm as mentioned in Chapter 1.
4.3.3 Improvement through sequential queries

Experience with the dihedral group using parallel queries, for which an NP-complete problem needs to be solved in its average case form, indicates that the answer to this problem lies perhaps in a different direction. Like the dihedral group requiring the solution of the subset sum problem, there is a host of groups requiring the solution of some “matrix sum problem” [25]. One presents the queries in a sequential manner, so that there is a “learning process” from one stage to the next. The Hilbert space is $\mathbb{C}[G] \otimes \mathbb{C}[X]$. This paradigm can be described by the following diagram:

$$E \underbrace{O_f U_m \ldots O_f U_1 O_f \Psi}_{m \text{ times}}$$

where $\Psi$ is a query, $\{U_i\}$ are arbitrary unitary operations and $E$ is a measurement. Then the search is for a set of $\Psi$, $\{U_i\}$, and $E$ such that the subgroups can be distinguished with maximum probability. Preliminary results indicate that this idea is promising for the case of dihedral group of order 6, the simplest case. This approach can possibly circumvent the subset sum problem for the dihedral group and perhaps more generally matrix sum problems, albeit requiring a different way of thinking than that for parallel queries. The query selection methodology influences and guides the thinking for this approach and helps to develop it.

With $m = 1$, i.e., with a single unitary operator and two uses of the oracle, it turns out that the HSP over dihedral group of order 6 can be solved with probability 1 if the response space $X = \mathbb{Z}_3$. We start with the character query $\Psi = |\chi_1\rangle$ (choice influenced by single-query optimization). Define the sets $S_k := \{O_f U_1 O_f \Psi : f \text{ hides } H_k\}$. Let $V_k = \text{span}(S_k)$. The approach is to find some $U_1$ such that $\{V_k\}_{k \in X}$ are orthogonal subspaces.

This condition gives a set of polynomial conditions in the entries of $U_1$. The technique of Gröbner basis yields the solution, and hence $U_1$. Once this is known the PGM can be applied (due to the symmetry in the problem) to obtain the optimal measurement. This technique does not scale well with the size of the problem, making analysis that much harder.
4.4 Future direction

We conclude this chapter and the thesis with the following remarks about the future direction of research in this area. Through the single-query optimization and the work on dihedral group PGM implementation, the central role of representation theory in HSP algorithms has been demonstrated.

The dihedral PGM implementation brings forth the importance of finding the transformation to the correct representation bases. Moreover, the final implementation of the measurement is also dependent on getting the Naimark embedding via implementable transforms. The techniques that surface in this part of the investigation are potentially useful in other such problems.

The investigation of queries as a tool towards improving the HSP algorithms is a promising area with room for significant development. In this chapter we have seen how dramatically the success probability improves by altering the queries. We would like to find a general framework for at least a class of queries for the multi-query case. This looks possible in some cases, but in general would be an involved problem because of the reasons stated at the end of section 4.1.

The order in which we plan to examine the queries in future work follows the order of the presentation above. We give a map and propose some of the computations that would need to be done to develop the multi-query results. First the unentangled character query, followed by the entangled character queries. Finally the sequential queries can be considered.

For an analytical approach, of use is the fact that \( (\otimes^2 O_f) |\Psi^2\rangle ) (4.6) \) is \( H_k^{\times 2} \) invariant for the oracle hiding \( H_k \). This, coupled with the fact that the oracle functions are permutations, should allow the mixed state \( \rho^2_{k,(y_1,y_2)} \) (4.7) to be specified. Then the computation of the PGM can be done for the purpose of proving its optimality (if it is indeed optimal). Further, a structure of the general \( \rho^2_{k,\vec{v}} \) (4.3) for the case for an abelian response space \( X \) may become clear, leading to assertions about the success probability, or the commonality of optimal measurements as in the single-query case.

The entangled query is more complicated since it has a diagonal term in its queried state \( (\otimes^2 O_f) |\Psi_D\rangle \). This is not an invariant of the \( H_k^{\times 2} \) translation, but
of $H_k$ acting diagonally on the tensor product space \( \bigotimes^2 \mathbb{C}[G] \). Since the entangled query is derived from the unentangled query by subtracting a term proportional to the diagonal through the parameter $t$ (4.8), it must be possible to find the optimal value $t^*$ of this parameter to maximize the success probability by considering extension of the unentangled state $\rho_k^{(y_1,y_2)}$ through a Naimark-like embedding. This is to be investigated using ideas that are in principal akin the to recent work in [32], that of decoding a second-order Reed-Muller code to improve the decoding probability.

Investigation of sequential queries is, as stated before, an idea to possibly get around the subset-sum like problems, but as is clear from the formulation, the intermediate unitary transformations $U_i$ will certainly make the query state into a state which is not an equal superposition over the group. The representation theory based approach becomes harder to apply, and the formulation may have to involve optimization techniques from general matrix methods in conjunction with the Gröbner basis as in the example.

We conclude that within the outlines mentioned, there are a variety of possible directions and some breadth of problems yet to be resolved, with parallels in other areas of research.
Bibliography


Appendix A

The left translation representation of the dihedral group

Consider the dihedral group, $G$, of order $2N$. As a set:

$$G = \{(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_N\}$$

with the semi-direct product defined to be:

$$(x', y') \cdot (x, y) = (x + x', (-1)^{x'} y + y')$$

For $\phi \in \mathbb{C}[G]$, left translation by $g'$ is given as:

$$L(g')\phi(g) = \phi(g'^{-1} g).$$

Let

$$g' = (x', y'), \; \text{so} \; g'^{-1} = (-x', -(1)^{x'} y')$$

$$g = (x, y)$$
then
\[ L(g')\phi(g) = \phi \left( (x + x', (-1)^{x'}(y - y')) \right) \]

Since \( G \) is set theoretically \( \mathbb{Z}_2 \times \mathbb{Z}_N \) we have:

\[ \mathbb{C}[G] \cong \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_N] \]

We introduce the computational basis of \( \mathbb{C}[\mathbb{Z}_N] \) consisting of the \( \delta \) functions

\[ \delta_y(y') = \begin{cases} 1 & \text{if } y' = y \\ 0 & \text{if otherwise} \end{cases} \]

with \( |y\rangle := \delta_y \). Similarly for \( \mathbb{C}[\mathbb{Z}_2] \).

\[ \delta_x(x') = \begin{cases} 1 & \text{if } x' = x \\ 0 & \text{if otherwise} \end{cases} \]

with \( |x\rangle := \delta_x \). Thus we can choose \( \mathbb{C}[G] \) computational basis to be the elements:

\[ |x, y\rangle \leftrightarrow |x\rangle |y\rangle \]

The left translation representation of \( G \) is given as:

\[ L(g') = \tau_2(g') \otimes \tau_N(g') \] (A.1)

\[ \tau_2(g')\gamma(x) = \gamma(x + x'), \quad \text{where } \gamma \in \mathbb{C}[\mathbb{Z}_2] \]

\[ \tau_N(g')\varphi(y) = \varphi \left( (-1)^{x'}(y - y') \right), \quad \text{where } \varphi \in \mathbb{C}[\mathbb{Z}_N] \]

We examine the unitary representation of \( G \); \( (\tau_2, \mathbb{C}[\mathbb{Z}_2]) \). Let the characters of \( \mathbb{C}[\mathbb{Z}_2] \) be \( \{ |\zeta_\nu\rangle \}_{\nu \in \mathbb{Z}_2} \):

\[ \zeta_\nu(x) = \frac{1}{\sqrt{2}} (-1)^{\nu x} \]

Then \( (\tau_2, \mathbb{C}[\mathbb{Z}_2]) \) splits up as two one-dimensional representations under the left
translation action $\tau_2$

$\mathbb{C}[Z_2] = \mathbb{C}\zeta_0 \oplus \mathbb{C}\zeta_1$

$(\tau_N, \mathbb{C}[Z_N])$ also defines a unitary representation of $G$. Let us examine it in terms of sub-representations.

Let $\omega = e^{2\pi i/N}$. Then $Z_N$ has $N$ one dimensional characters, $\{|\chi_\mu\rangle\}_{\mu \in \mathbb{Z}_N}$, defined by:

$$\chi_\mu(y) = \frac{1}{\sqrt{N}} \omega^{\mu y}$$

For $\mu \in \{1, \ldots, \lfloor \frac{N-1}{2} \rfloor \}$, let us denote by $V^\mu$ the subspace of $L^2_0(Z_N)$ spanned by $\chi_{-\mu}$ and $\chi_\mu$:

$$V^\mu := \mathbb{C}|\chi_{-\mu}\rangle \oplus \mathbb{C}|\chi_\mu\rangle$$

Then each $V^\mu$ for $\mu \in \{1, \ldots, \lfloor \frac{N-1}{2} \rfloor \}$ constitutes an irreducible 2-dimensional representation of $G$ under the left translation action $\tau_N$ restricted to $V^\mu$.

Also define a 1-dimensional space of equal superposition states:

$$V^0 := \mathbb{C}\chi_0$$

$$\mathbb{C}[Z_N] = V^0 \oplus \bigoplus_{\mu \in \{1, \ldots, \lfloor \frac{N-1}{2} \rfloor \}} V^\mu$$

We define the spaces:

$$W^{(\nu,\mu)} := \begin{cases} 
\mathbb{C}|\zeta_\nu\rangle \otimes V^0, & \text{if } (\nu, \mu) \in Z_2 \times \{0\} \\
\mathbb{C}|\zeta_\nu\rangle \otimes V^\mu, & \text{if } (\nu, \mu) \in Z_2 \times \{1, \ldots, \lfloor \frac{N-1}{2} \rfloor \}
\end{cases}$$

Using (A.1) we can show (by comparing the characters of the representations) that the two-dimensional representations (for the restriction of $L = \tau_2 \otimes \tau_N$ (A.1)):

$$W^{(0,\mu)} \cong W^{(1,\mu)}, W^{(\nu,\mu)} \ncong W^{(\nu,\mu')} \text{ for } \mu \neq \mu' \in \{1, \ldots, \lfloor \frac{N-1}{2} \rfloor \}$$

Odd $N$:

Then the dimension count gives: $(N - 1)/2 \times 4 + 2 = 2N$. So we have described
up to equivalence all irreducible unitary representations of $G$. This implies:

$$\mathbb{C}[G] = \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_N] = \bigoplus_{\{(\nu, \mu)\}} W^{(\nu, \mu)}$$  \hspace{1cm} (A.2)

**Even $N$:**

Additionally, when $N$ is even we define another 1-dimensional subspace spanned by the character $|\chi_{N/2}\rangle$:

$$V_{N/2} := \mathbb{C}|\chi_{N/2}\rangle$$

$$\mathbb{C}[\mathbb{Z}_N] = V^0 \oplus V_{N/2} \oplus \bigoplus_{\mu \in \{1, \cdots, N/2-1\}} V^\mu$$

We define the spaces:

$$W^{(\nu, \mu)} := \begin{cases} 
\mathbb{C}|\zeta_\nu\rangle \otimes V^0, & \text{if } (\nu, \mu) \in \mathbb{Z}_2 \times \{0\} \\
\mathbb{C}|\zeta_\nu\rangle \otimes V_{N/2}, & \text{if } (\nu, \mu) \in \mathbb{Z}_2 \times \{N/2\} \\
\mathbb{C}|\zeta_\nu\rangle \otimes V^\mu, & \text{if } (\nu, \mu) \in \mathbb{Z}_2 \times \{1, \cdots, \lfloor N/2 \rfloor\} 
\end{cases}$$

The dimension count gives: $(N/2 - 1) \times 4 + 4 = 2N$. So we have described up to equivalence all irreducible unitary representations of $G$. This implies:

$$\mathbb{C}[G] = \mathbb{C}[\mathbb{Z}_2] \otimes \mathbb{C}[\mathbb{Z}_N] = \bigoplus_{\{(\nu, \mu)\}} W^{(\nu, \mu)}$$

This completes the decomposition of $\mathbb{C}[G]$ for the left translation representation.