Hidden Subgroup Problem - About some classical and quantum algorithms.

Maria Perepechaenko

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science Mathematics and Statistics[1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

[1] The M.Sc. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

Most quantum algorithms that are efficient as opposed to their equivalent classical algorithms are solving variants of the Hidden Subgroup Problem (HSP), therefore HSP is a central problem in the field of quantum computing. In this thesis we offer some interesting results about the subgroup and coset structure of certain groups, including the dihedral group. We describe classical algorithms to solve the HSP over various abelian groups, and the dihedral group. We also discuss some existing quantum algorithms to solve the HSP, and give our own novel algorithms and ideas to approach the HSP for the dihedral groups.

Acknowledgements

First and foremost, I would like to thank my supervisor, Dr. Monica Nevins, who first suggested the study of the Hidden Subgroup Problem. Her kindness, encouragement, wisdom, and trust in my abilities as a researcher have been invaluable during my graduate studies. She has become a true inspiration and mentor for me over the last few years. I am thankful for her ability to recognize my strengths and weaknesses as a mathematician and help me grow both academically and personally.

I am grateful to my thesis committee, Dr. Jason Crann and Dr. Gary Walsh for their time and feedback on my MSc thesis. I also want to thank them for the helpful courses they taught me, and the interesting discussions we had during my graduate studies. I would like to thank Dr. Anne Broadbent for always having her door open for me if I ever had a question. I am grateful to Sébastien Lord, for our correspondence and discussions in the moments when I was stuck and needed feedback on some of my ideas.

A huge thank you goes to the staff at the Department of Mathematics and Statistics, especially to Dr. Benoit Dionne and Diane Demers, for all the hard work they have been doing, their support and kindness.

I would also like to thank QUASAR members for the many interesting talks and events organized.

I thank my office-mates, who have become my dear friends, Masoomeh Akbari, Samuel Pilon, Jérémy Champagne, and Trinity Chinner for the countless hours of fun discussions, laughs, and great advice when it comes to math.

This thesis would not have been possible without my family, who made it possible for me to study and thrive in Canada. Especially, I would like to thank my mom for being my biggest cheerleader for the last eight years. I would also like to thank my dear husband, Efe, for his incredible support. He has driven a total of twenty thousand kilometres to see me once a month in Ottawa. His love and support have given me strength during tough times.

Lastly, I would like to thank Sectigo Inc. for their sponsorship. In particular, I would like to thank Jason Soroko, for always being in touch with me despite his busy schedule.

Contents

1 Introduction **1**

2 Classical algorithms for the HSP **5**

2.1 Hidden Subgroup Problem 5

2.2 Background 9

2.2.1 Floors, ceilings and binary search 9

2.2.2 Group theory 12

2.3 Classical query complexity of the Hidden Subgroup Problem for abelian groups 15

2.3.1 The case of $\mathbb{Z}/p^n\mathbb{Z}$, for a prime p. 16

2.3.2 The case of general cyclic group $\mathbb{Z}/N\mathbb{Z}$ 17

2.3.3 The case of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, for a prime p. 24

2.3.4 The case of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$, for a prime p. 31

2.4 Classical algorithms for the dihedral groups 35

2.4.1 Dihedral groups 35

2.4.2 The case of D_{2n} for various n. 39

3 Quantum algorithms for the HSP **45**

3.1 Background 45

3.1.1 Representation theory of finite groups 45

3.1.2 Quantum computing 53

3.2 Quantum Fourier Transform 59

3.2.1 Quantum Fourier Transform: abelian groups 59

3.2.2 Quantum Fourier Transform: general groups 61

3.3 Coset sampling method 63

3.3.1 Standard method 64

3.3.2 Standard method for finite abelian groups 66

3.3.3 Standard method for general groups 70

4 Dihedral HSP **71**
4.1 Dihedral group 71
4.2 Standard method 73
4.2.1 Dihedral Standard Method 73
4.2.2 Effect of change of basis on the standard method 75
4.3 Greg Kuperberg's algorithm with $n = 2^m$ 77
4.4 Novel algorithms 80
4.4.1 DHSP and the Phase estimation algorithm 80
4.4.2 Collapsing a perfect superposition to a known chosen state . 83
4.4.3 Additional results 90
4.4.4 Coset tensors algorithm 91

Chapter 1

Introduction

When studying quantum computing or simply reading articles about quantum computers, one would certainly come across Shor's algorithm, Simon's algorithm, and other "exponentially fast" quantum algorithms. All of these algorithms fall under the framework of the Hidden Subgroup Problem (HSP). Indeed, most quantum algorithms that run exponentially faster than equivalent deterministic or probabilistic classical algorithms are doing so by solving special instances of the HSP [19]. So the HSP is central in the field of quantum computing.

In large, the HSP is a problem of finding the unknown period of a periodic function, whose domain has a very complex and detailed structure. The formal definition of the HSP is as follows.

Definition (Definition of the HSP)**.** Let G be a group, and let H be a subgroup of G. Given a finite set X, and a function $f : G \to X$ such that f is constant on left cosets of H and distinct on distinct cosets, find H.

Classical query complexity of the HSP is known [11]. Moreover, there exists an efficient quantum algorithm to solve the abelian hidden subgroup problem [17, 11]. However, the best known quantum algorithm to solve the HSP over a certain instance of non-abelian groups, a dihedral group, is still subexponential [14, 15, 21]. We do not know of any efficient quantum algorithms to solve the HSP over any arbitrary finite group. This thesis aims at studying the HSP over both abelian and non-abelian groups in the classical and quantum setting, with special attention paid to the Dihedral hidden subgroup problem.

This thesis is broken into three parts. In the first part we focus on the classical HSP. We state some useful and interesting results about the subgroup and coset structure of certain abelian groups. We then use these results to give classical algorithms to solve the HSP over $G = \mathbb{Z}/N\mathbb{Z}, G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, and $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$, for positive integer N, and prime p, and discuss their complexity. We also give a remark regarding the case $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$, for some positive integer k. We then shift our attention to the case $G = D_{2n}$. We state some results about the subgroup structure of D_{2n}, and describe classical algorithms to solve the HSP over $G = D_{2p}, D_{2p^k}$, and D_{2n}, for some positive prime p, and positive integer n.

In the second and third parts of the thesis we leave the "classical world", and look into the quantum algorithms to solve the HSP. In the second part, we discuss the Quantum Fourier Transform for abelian, and then general groups in terms of representation theory, and describe the standard method to solve the HSP over abelian and non-abelian groups.

In the third part, we focus solely on the Dihedral HSP. We state some useful representation theory results for D_{2n}. We describe the standard method to solve the HSP over D_{2n}, as well as the effect of the change of basis on the standard method. We also discuss the existing quantum algorithm by Greg Kuperberg for the case $D_{2^{m+1}}$ [14]. We then propose some novel algorithms to solve the Dihedral HSP. Unfortunately, our algorithms are not efficient. However, we discuss some very interesting ideas for a possible efficient quantum algorithm to solve the HSP over D_{2n}. In particular, we discuss an algorithm from [25], that transforms a perfect superposition to a known state, and attempt to redesign the algorithm in order to solve the HSP. Regrettably, there is a subtlety that prevents the algorithm from working the certain way we want. Nevertheless, we provide an interesting discussion, in attempts to inspire research focused on new algorithms to solve the Dihedral HSP.

The classical algorithms in this thesis are original. To the author's knowledge there are no research papers explicitly giving classical algorithms to solve the HSP over these groups, although the authors of [12, Section 3.2] briefly mention the query complexity of the HSP over cyclic groups. The algorithms in Section 4.4 are original, and have been inspired by [1, 5, 6, 9, 13, 18], and many encouraging conversations with Dr. Nevins.

A brief overview of related literature

We chose the focus of this thesis to be on the Dihedral HSP due to its applications to post-quantum cryptography. It was Oded Regev who first discussed the connection between the Dihedral HSP and certain lattice problems [20]. He showed a reduction from the poly(n)-unique Shortest Vector Problem(SVP) to the Dihedral HSP, and that if there is an algorithm solving the Dihedral HSP by coset sampling method, this algorithm would efficiently solve the the poly(n)-unique SVP. Thus, solving the HSP presents a possible threat to certain lattice-based encryption schemes.

There has been a lot of research focused on the HSP. So far, the best-known algorithm to solve the HSP over dihedral groups is due to Greg Kuperberg. Unfortunately, the algorithm requires a subexponential number of queries. Mark Ettinger and Peter Høyer in [6] gave an algorithm to solve the HSP over a finite general group G, that uses only polynomial number of calls to the oracle. However, their algorithm requires exponential time. Yoshifumi Inui and Francois Le Gall, presented an efficient quantum algorithm solving the HSP over groups of the form $G_{p,r} = \langle x, y \mid x^{p^r} = y^p = e, yx = x^{p^{r-1}+1}y\rangle$, for prime p, and $r \geq 2$, except $p = r = 2$ [12]. Dave Bacon et. al. showed that $\Omega(\log |G|)$ hidden subgroup states are necessary to solve the hidden subgroup problem [1].

In their paper Dave Bacon et. al. have also explored the connections between the dihedral hidden subgroup problem and average case subset sum problems (SSP). Oded Regev has shown that if one can efficiently solve $\frac{1}{poly(\log_2 n)}$ of the legal subset sum inputs, given at least $\log_2 n + 4$ number of copies of the coset state, then there is an efficient quantum algorithm for the DHSP [20]. Despite the general SSP being NP-hard, an algorithm for the average-case inputs, with at least $\log_2 n + 4$ number of copies of the coset state, would be sufficient to solve the DHSP [1]. Greg Kuperberg is using a special sieve to create a desirable state in order to conclude the parity of the shift of the hidden reflection. Another way is to view this as a subset sum problem.

Recently, there has been tremendous progress in the research focused on the SSP. Xiao-Yun Xu et. al. presented a chip built-in photonic computer efficiently solving certain instances of the subset sum problem [24]. Their work suggests that the photonic computer might be able to efficiently solve SSP in general. Yang Li and Hongbo Li proposed a new quantum algorithm, with heuristic time and memory complexity $2^{0.209n}$, up to polynomial factors [16]. This result is a significant improvement of the result due to Bernstein [2] $2^{0.241n}$, up to polynomial factors, and later due to Helm and May [10] $2^{0.226n}$, up to polynomial factors. Thus, it might be possible that the solution to the DHSP will emerge from the work on the SSP. Being the central problem in quantum computing, we may expect the solution to the HSP to arrive from a very unexpected direction.

Detailed overview of the thesis

In Chapter 2 we talk about classical algorithms for the HSP. In Section 2.1 we state the problem. We state and prove the classical query complexity of the HSP over an arbitrary group G. We also give an algorithm to solve the HSP under certain hypothesis. In Section 2.2 we give some useful background results that will later be used to prove the main results of this thesis. In Section 2.3 we state and prove results about the subgroup and coset structure of some abelian groups, and describe quantum algorithms to solve the HSP over various abelian groups. Section 2.4 is dedicated to classical algorithms over dihedral groups. In this section we state and prove some observations regarding subgroup structure of the dihedral groups, and give classical algorithms to solve the HSP over D_{2n}, for various n.

In Chapter 3, we talk about quantum algorithms to solve the HSP. We provide some representation theory and quantum computing background in Section 3.1. We discuss the Quantum Fourier Transform for both abelian and general groups in Section

3.2. In the Section 3.3 we describe the coset sampling method to solve the HSP over finite abelian and finite general groups.

In Chapter 4, we focus on the Dihedral HSP. In Section 4.1 we state some results on representation theory for the dihedral groups. In Section 4.2 we describe standard method to solve the HSP over dihedral groups, as well as the effect of the change of basis on the standard method. We dedicate Section 4.3 to the quantum algorithm to solve the Dihedral HSP by Greg Kuperberg. In Section 4.4 we describe some novel quantum algorithms to solve the Dihedral HSP, including an algorithm mimicking that in paper by Ahmed Younes et.al. on collapsing the superposition to a known state, and a new approach using “coset tensors” in place of coset states.

Chapter 2

Classical algorithms for the Hidden Subgroup Problem

2.1 Hidden Subgroup Problem

Let us begin by defining the problem that we will be working on for the rest of this text. Let us also start off our search for the best possible attack on the Hidden Subgroup Problem (HSP) by looking at the lower bound of the classical query complexity of the HSP for any group G.

Definition 2.1.1. Let G be a finite group and H be a subgroup of G. Let X be a finite set. A function $f : G \mapsto X$ is said to be strictly H-periodic if it is constant on left cosets of H and distinct on distinct cosets of H.

Example. Let $G = \mathbb{Z}/6\mathbb{Z}$. Let $H = \langle 2 \rangle$. Let $f : G \mapsto X$, where $X = \{a, b\}$, such that $f(0) = f(2) = f(4) = a$ and $f(1) = f(3) = f(5) = b$. Then we say that the function is H-periodic, since it is constant on the cosets of H and distinct on distinct cosets.

Hidden Subgroup Problem (HSP). *Given a description of a group G, a subgroup $H \leq G$ and a finite set X, as well as a strictly H-periodic function $f : G \mapsto X$, find a generating set for H.*

Example. Similar to the previous example, let $G = \mathbb{Z}/8\mathbb{Z}$. Let $H = \langle 4 \rangle$. Let $X = \{a_1, a_2, a_3, a_4\}$. Suppose that $f : G \mapsto X$ is an H-periodic function. The goal is to find H. A very unexciting attack would be the one that requires querying elements of the group G, by which we mean evaluating the function on the elements of G, one by one until it is possible to unveil the hidden subgroup H. Since we know that the identity element $0_G = 0$ is always in H, it would make sense to start by querying $f(0)$ and then query all the remaining elements to match their functional values to $f(0)$. Such attack will take at most $|G| = 8$ queries.

There are possibly more sophisticated approaches to find H. Perhaps, one way to solve the HSP in this case would be to query the identity and generators of the nontrivial subgroups of G. Since H is either $\langle 2\rangle$, $\langle 4\rangle$, $\langle 0\rangle$, or G. It would suffice to make three queries $f(0), f(2), f(4)$ in order to learn what H is.

Note that you could be very lucky and query all the right elements one by one entirely by luck, and get the hidden subgroup H in merely a few queries. In this text we will not account for such cases. We will consider what we call the "worst case" scenario which implies that there is absolutely no lucky queries and one needs to use all their resources and clever queries to find H.

In this text we use the term oracle or black-box function, to describe a machine or a function that we can only view in terms of its inputs and outputs, without any knowledge of its internal workings, and in case of a function of how it assigns values.

The following theorem is relatively well-known; see for example [3, Theorem 5.1].

Theorem 2.1.2 (Classical query complexity of HSP)**.** *Let G be a group and suppose that G has a set $\mathcal{H}$ of N nontrivial subgroups whose only common element is the identity. Then in the worst case the number of queries a classical computer must make to solve HSP is at least $\sqrt{2N}$.*

To understand the proof better imagine yourself at a party. A friend of yours suggested a game of battleship that has special rules. He will only draw one ship but he can change the location of the ship whenever necessary as you make your "shots". When there are no more available positions for him to take he will admit defeat and tell you the position of his ship.

Proof: Assume that the oracle does not hide a particular subgroup H, but rather is playing the battleship game by hiding a different subgroup H whenever necessary. On the t-th query, the algorithm takes a group element g_t as an input that we assume is different from all previous queries $g_0, \dots, g_{t-1}$ and outputs t, if the game is still ongoing it must be that $f(g_i) \neq f(g_j)$, for any $i \neq j \in \{0, \dots, t\}$. If on the t-th query $f(g_t) = f(g_i)$ for some i in the set $\{0, \dots, t-1\}$, then the oracle is forced to concede if and only if it provides enough information to determine the hidden subgroup. In this case, we want to know what can be said about t.

Notice that we can take advantage of the following property:

$$f(g_i) = f(g_j) \text{ if and only if } g_iH = g_jH \text{ if and only if } {g_j}^{-1}g_i \in H.$$

So before the t-th query each such element ${g_j}^{-1}g_i$ was an element of some $H' \in \mathcal{H}$ such that $H' \neq H$. After the t-th query there were at most $\binom{t+1}{2}$ distinct elements of the form ${g_j}^{-1}g_i$, where $i, j \in \{0, \dots, t\}$. Since the oracle was forced to stop cheating, that means that the oracle was unable to find a new group other than H that contains a new element of the form ${g_j}^{-1}g_i$, where $i, j \in \{0, \dots, t\}$. In other words, there were more elements of the form ${g_j}^{-1}g_i$ than available groups in the set $\mathcal{H}$. Since there were at most $\binom{t}{2}$ such elements and at most N groups we must have $\binom{t}{2} \geq N$.

This inequality could be simplified since $\binom{t+1}{2} = \frac{(t+1)!}{(t-1)!2!} = \frac{(t+1)t}{2} \geq N$, yielding $t \geq \sqrt{2N}$. ∎

As we have shown in the example above, there is a so-called "brute-force attack" that simply requires querying elements of the group G one by one until it is possible to unveil the hidden subgroup H. Such attack will take at most $|G|$ queries. Thus, the complexity of an average attack is anywhere between $\sqrt{2N}$ and $|G|$. Now that we have seen the result of the Theorem 2.1.2, we will aim to find a classical attack that takes approximately $\sqrt{2N}$, for a group G that has N nontrivial subgroups whose only common element is the identity. The closer we get to the lower bound in the theorem 2.1.2, the finer our attack is.

We now establish a lemma about abelian groups inspired by the strategy of the proof above. If g is an element of a group G, we denote by $\langle g\rangle$ the subgroup that it generates.

Lemma 2.1.3. *Let G be a finite abelian group and set $g_0 = e$. Suppose that there exists a sequence $\{g_1, \cdots, g_n\}$ of n additional elements of G such that for each $i \in \{1, \ldots, n\}$ we have*

$$g_i^m \notin g_\ell \langle g_j^{-1} g_k \rangle \tag{2.1.1}$$

for all $0 \leq j, k, \ell < i$, and for all $1 \leq m < ord(g_i)$. Then the $n(n+1)/2$ cyclic subgroups

$$K_{j,k} = \langle g_j^{-1} g_k \rangle, \quad \textit{for all } 0 \leq j < k \leq n$$

of G are distinct.

Proof: The statement is true if $n = 0$, as there is only one subgroup (the trivial subgroup) in the list.

Suppose the subgroups $K_{j,k}$, as j and k range over the set $0 \leq j < k \leq n-1$, are all distinct. We need to show that the subgroups $K_{j,n}$, as j ranges over the set $0 \leq j < n$, are all distinct and distinct from the preceding subgroups.

Suppose to the contrary that $\langle g_j^{-1} g_n\rangle = \langle g_k^{-1} g_\ell\rangle$ for some $0 \leq j < n$ and $0 \leq k < \ell < n$. Then in particular $g_n \in g_j K_{k,\ell}$, which contradicts 2.1.1.

Now suppose to the contrary that $\langle g_j^{-1} g_n\rangle = \langle g_i^{-1} g_n\rangle$ for some $0 \leq i \neq j \leq n$. Then there exists some $m \in \mathbb{N}$ such that $g_j^{-1} g_n = (g_i^{-1} g_n)^m = g_i^{-m} g_n^m$, where the second equality follows since G is abelian. If $g^{1-m} = e$ then we deduce that $g_j \in \langle g_i\rangle$, a contradiction. Otherwise, $g_n^{1-m} = g_j g_i^{-m} \in g_j\langle g_i^{-1}\rangle$, again a contradiction.

Therefore the $n(n+1)/2$ subgroups $K_{i,j}$, with $0 \leq i < j \leq n$, are distinct. ∎

We now apply this lemma to give an efficient algorithm to solve the HSP under certain hypotheses.

Theorem 2.1.4. *Let G be a finite abelian group that has M distinct nontrivial cyclic subgroups. Let $n = \lfloor \frac{-1+\sqrt{1+8M}}{2} \rfloor \in \mathbb{N}$, and suppose that there is a sequence $\{g_0, g_1, \cdots, g_n\}$ of elements of G satisfying the hypothesis of Lemma 2.1.3. Then there exists an attack of complexity $O(\sqrt{M})$ to find any hidden cyclic subgroup of G.*

Proof: Let $\{g_0, g_1, \cdots, g_n\}$ be a sequence of elements of G satisfying the hypotheses of Lemma 2.1.3. Then the $n(n+1)/2$ subgroups given by

$$K_{i,j} = \langle g_i^{-1} g_j \rangle, \quad \text{with } 0 \leq i < j \leq n$$

are distinct. Then by hypothesis G has an additional

$$t = M - \frac{1}{2}n(n+1) \leq \frac{1}{2}(n+1)(n+2) - \frac{1}{2}n(n+1) = n+1$$

cyclic subgroups. Choose generators $h_1, \ldots, h_t$ for these t subgroups.

Now suppose H is a hidden subgroup of G which is cyclic and let f be a hiding function. Our attack is as follows. Query each element of the set $\{g_0, g_1, \cdots, g_n, h_1, \cdots, h_t\}$. Then analyse the results as follows.

Since H is among the N listed subgroups, it is either equal to $K_{i,j}$ for some $0 \leq i < j \leq n$ or equal to $\langle h_i \rangle$ for some $1 \leq i \leq t$. If $H = K_{i,j}$ then $g_i^{-1} g_j \in H$ so $g_i H = g_j H$ and so $f(g_i) = f(g_j)$. If $H = \langle h_i \rangle$ then $h_i \in H$ so $f(h_i) = f(g_0)$ where $g_0 = e$ by hypothesis.

Conversely, if $f(g_i) = f(g_j)$ for some $i < j$ then $g_i H = g_j H$ so $g_i^{-1} g_j \in H$. This implies that $K_{i,j} = \langle g_i^{-1} g_j \rangle \subset H$, but in general it may fail to be an equality, if the cyclic subgroups are not of prime order. On the other hand, if $f(h_i) = f(g_0)$ then necessarily $H = \langle h_i \rangle$. Therefore we recover H in all cases as the union of all the subgroups $K_{i,j}$ such that $f(g_i) = f(g_j)$ and all the subgroups $\langle h_i \rangle$ such that $f(h_i) = f(g_0)$.

The query complexity of this attack is $n + 1 + t \leq 2n + 2$, where by hypothesis n is $O(\sqrt{M})$. ∎

Note that in case when all the cyclic subgroups have prime order, the condition (2.1.1) reduces to $g_n \notin g_j \langle g_k^{-1} g_\ell \rangle$, for all $0 \leq j, k, \ell < i$.

Example. Let $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $H = \langle (1,1) \rangle$ be the hidden subgroup. Note that G has four nontrivial cyclic subgroups, namely $K_1 = \langle (0,1) \rangle, K_2 = \langle (1,0) \rangle$, $K_3 = \langle (1,1) \rangle$, and $K_4 = \langle (1,2) \rangle$. We will try to use technique from Theorem 2.1.4 in order to find H.

First, query $\{g_0 = (0,0), g_1 = (0,1), g_2 = (1,0)\}$ such that all g_0, g_1 and g_2 satisfy the hypothesis of Lemma 2.1.3. Now we need to check whether any of these queries are equal. Suppose that none of them are equal. This tells are that H is not the whole group. Moreover, that $H \neq K_1$, $H \neq K_2$, and $H \neq \langle g_2 - g_1 \rangle = K_4$.

Note that we can not conclude what H is yet, as there are two more choices for H, namely K_3 and the trivial subgroup. We also can no longer query g_3, such that $g_3 \notin g_m\langle g_k - g_l \rangle$, for all $0 \leq k, l, m < 3$.

Now the most obvious course of action would be to query $h_1 = (1,1)$ to decide whether H is equal to K_3 or the trivial subgroup.

Remark 2.1.5. The hypothesis in this theorem is not always satisfied. It may happen that a given sequence of elements $\{g_0, g_1, \cdots\}$ cannot be completed to a sequence of the necessary length n.

If the cyclic subgroups of G intersect only trivially, then $M = N$ and this bound is of optimal complexity.

2.2 Background

Before we dive in the main component of the first part of this text, let us establish some background. Classical algorithms to solve the HSP require certain results from combinatorics, and most importantly from the group theory. We will establish some group theory background after necessary results from combinatorics. The reader might find some of the theory to be quite elementary. Nevertheless, we decided it to be more convenient to have any necessary theory on hand available for the reader at any time.

2.2.1 Floors, ceilings and binary search

Definition 2.2.1. The floor of a real number x is the greatest integer m s.t. $m \leq x$. We denote it by $\lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\}$. The ceiling of a real number x is the smallest integer k s.t. $k \geq x$. We denote it by $\lceil x \rceil = \min\{k \in \mathbb{Z} : k \geq x\}$.

Lemma 2.2.2. *Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. Then $x \leq n$ iff $\lceil x \rceil \leq n$.*

Proof: Let $x \leq n$. Since n is an integer, $\lceil x \rceil \leq n$. Let $\lceil x \rceil \leq n$, then the following inequality is true: $x \leq \lceil x \rceil \leq n$. Thus, $x \leq n$. ▮

Lemma 2.2.3. *For all $x \in \mathbb{R}$ and $n \in \mathbb{Z}$, $\lceil x + n \rceil = \lceil x \rceil + n$.*

Proof: Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. From the definition of the ceiling function $x \leq \lceil x \rceil < x + 1$. Thus, $x + n \leq \lceil x \rceil + n < x + n + 1$. Since $\lceil x \rceil = n$ if and only if $x \leq n < x + 1$, we conclude that $\lceil x \rceil + n = \lceil x + n \rceil$. ▮

Lemma 2.2.4. *Let $k \in \mathbb{Z}$ and $k \geq 0$. Then $k - \lceil \frac{k-1}{2} \rceil > \lceil \frac{k-1}{2} \rceil$.*

Proof: Assume for contradiction, that $k - \lceil \frac{k-1}{2} \rceil \leq \lceil \frac{k-1}{2} \rceil$. Then $k \leq 2\lceil \frac{k-1}{2} \rceil$. Since $2\lceil \frac{k-1}{2} \rceil = \lceil \frac{2(k-1)}{2} \rceil$, it follows that $k \leq \lceil k - 1 \rceil$. However, $k \in \mathbb{Z}$, thus $\lceil k - 1 \rceil = k - 1$. As a result we have that $k \leq k - 1$. This implies that $0 \leq -1$. Our assumption led to a contradiction that $0 \leq -1$. Hence, $k - \lceil \frac{k-1}{2} \rceil > \lceil \frac{k-1}{2} \rceil$. ▮

Lemma 2.2.5. *For an odd positive integer k, $\lceil \log_2 (k + 1) \rceil = \lceil \log_2 (k) \rceil$.*

Proof: Since $\log_2 x$ and the ceiling function are increasing functions, we can conclude that $\lceil \log_2 (k + 1) \rceil \geq \lceil \log_2 k \rceil$.

Now we will show that $\log_2 (k + 1) \leq \lceil \log_2 (k) \rceil$. Note that

$$k = 2^{log_2(k)} \leq 2^{\lceil \log_2 (k) \rceil}.$$

As a result, $\lceil \log_2 (k) \rceil$ is the least integer t s.t. $k \leq 2^t$. Given that k is odd, it can not be a power of two. Thus $k < 2^t$. On the other hand, k is an integer, so

$$k < k + 1 \leq 2^t.$$

Since $k + 1 \leq 2^t$, we note that $\log_2 (k + 1) \leq t = \lceil \log_2 (k) \rceil$. By Lemma 2.2.2 we deduce that $\lceil \log_2 (k + 1) \rceil \leq \lceil \log_2 (k) \rceil$.

We can conclude that for an odd k it is true that $\lceil \log_2 (k + 1) \rceil = \lceil \log_2 (k) \rceil$. ▮

For the purposes of our next few results let us recall what a totally ordered set is. A totally ordered set S is a set equipped with a relation R, for instance "$\leq$", that satisfies the following four conditions:

1. Reflexivity: $s \leq s$ for all s in S.

2. Transitivity: $s \leq t$ and $t \leq v$ implies $s \leq v$.

3. Antisymmetry: $s \leq t$ and $t \leq s$ implies $s = t$.

4. Comparability: For any s, t in S, either $s \leq t$ or $t \leq s$.

Example. Let S be a set of all subgroups of a group G ordered by inclusion. Then this set is not totally ordered since the first three conditions hold however, the comparability condition can fail.

Example. Let S be a set of all real numbers equipped with a relation $\leq$. Such a set S is totally ordered.

The backbone of the following theorem is the binary search algorithm. Let us recall that the binary search algorithm is a search algorithm that recursively finds the position of a target value within a totally ordered set by comparing the target value to the middle element of the set.

Theorem 2.2.6. *In the worst case, a binary search algorithm makes $\lceil \log_2 k \rceil$ queries to find the position of a target within a totally ordered set of a size k, where $k \geq 1$.*

Proof: Let S be a totally ordered set of k elements $S = \{s_1, s_2, s_3, \ldots, s_k\}$, containing the target element s_{target}. Let S be equipped with the relation that $s_{i-1} \leq s_i$, for $i \in \{2, \ldots, k\}$.

If $k = 1$, then the set S is a singleton so necessarily $S = \{s_{target}\}$. Therefore we will not perform any queries. Since $\lceil \log_2(1) \rceil = 0$, this proves the base case of our induction.

Let $k = n - 1$, and suppose that the result holds for all sets of size less than k. We query the middle element of the set, which is $s_{\lceil \frac{k+1}{2} \rceil}$. Notice that this query will efficiently divide the set into two halves, or almost halves.Notice that

$$\lceil \frac{k+1}{2} \rceil = \lceil 1 + \frac{(k-1)}{2} \rceil = 1 + \lceil \frac{(k-1)}{2} \rceil,$$

and, if $k \geq 2$, then $1 \leq \lceil \frac{(k-1)}{2} \rceil < \lceil \frac{k+1}{2} \rceil \leq k$. Thus the two halves are nonempty and are given by

$$S_1 = \{s_1, s_2, \ldots, s_{\lceil \frac{k-1}{2} \rceil}\}, \quad S_2 = \{s_{\lceil \frac{k+1}{2} \rceil}, \ldots, s_k\}.$$

Now we make a query: compare the value of s_{target} to the value of $s_{\lceil \frac{(k+1)}{2} \rceil}$.

If $s_{target} < s_{\lceil \frac{(k+1)}{2} \rceil}$, then $s_{target} \in S_1$.

If $s_{target} \geq s_{\lceil \frac{(k+1)}{2} \rceil}$, then $s_{target} \in S_2$.

By Lemma 2.2.4 we have the following inequality: $|S_2| = k - \lceil \frac{(k-1)}{2} \rceil > \lceil \frac{(k-1)}{2} \rceil = |S_1|$. Since $|S_2| < k$, we may apply the induction hypothesis to conclude that we need in total at most $Q = \lceil \log_2(k - \lceil \frac{(k-1)}{2} \rceil) \rceil + 1$ queries to identify the target element. Let us show that $Q = \lceil \log_2(k) \rceil$.

If k is odd, then $k - \lceil \frac{k-1}{2} \rceil = k - \frac{k-1}{2} = \frac{(k+1)}{2}$, and $\log_2((k+1)/2) = \log_2(k+1) - \log_2(2) = \log_2(k+1) - 1$.

Therefore

$$Q = \lceil \log_2(k - \lceil \frac{(k-1)}{2} \rceil) \rceil + 1 = \lceil \log_2(k+1) \rceil = \lceil \log_2(k) \rceil$$

by Lemma 2.2.4.

If k is even, then $k - \lceil \frac{(k-1)}{2} \rceil = k - \frac{k}{2} = \frac{k}{2}$ and $\log_2(k/2) = \log_2(k) - 1$ so

$$Q = \lceil \log_2(k - \lceil \frac{(k-1)}{2} \rceil) \rceil + 1 = \lceil \log_2(k/2) \rceil + 1 = \lceil \log_2(k) \rceil.$$

Therefore we can conclude that it takes at most $\lceil \log_2(k) \rceil$ queries to find s_{target} in a totally ordered set of size k for any integer $k \geq 1$.

▮

2.2.2 Group theory

The results in this subsection are fairly standard and are meant to aid one's memory if required. The textbook by Joseph Gallian [8] was consulted but the proofs are written by the author.

Lemma 2.2.7. *Let p be a prime. Let G be a group of order p. Then G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Proof: Let p be a prime and G be a group of order p. Let $e \neq g \in G$ be any element of the group except for the identity. Consider the subgroup $\langle g \rangle$. The order of $\langle g \rangle$ divides the order of G. But since the order of G is a prime, it implies that the order of $\langle g \rangle$ is either 1 or p. Since $g \neq e$, we conclude that $\langle g \rangle$ has order p. So G is a cyclic group of order p. Thus, G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. ▮

Lemma 2.2.8. *Let G be a group. Then there exists an isomorphism from G to $G \times \{1\}$, where $\{1\}$ denotes the trivial group.*

Proof: Let G be a group. Define $\phi : G \mapsto G \times \{1\}$ be a function $\phi(g) = (g, 1)$. Take any $g, g' \in G$. Note that $\phi(gg') = (gg', 1) = (g, 1)(g', 1) = \phi(g)\phi(g')$. Further, $\phi(1) = (1, 1) = 1_{G\times\{1\}}$. Therefore, ϕ is a homomorphism.

Define $\varphi : G \times \{1\} \mapsto G$ via $\varphi(g, 1) = g$. Take any $(g, 1)$ and $(g', 1) \in G$. Since $\varphi((g, 1)(g', 1)) = \varphi(gg', 1) = gg' = \varphi(g, 1)\varphi(g', 1)$ and $\varphi(1, 1) = 1 = 1_G$ we can conclude that φ is a homomorphism.

Finally, observe that $\varphi(\phi(g)) = g$ for any $g \in G$, and $\phi(\varphi(g, 1)) = (g, 1)$ for any $(g, 1) \in G \times \{1\}$. Hence, $G \cong G \times \{1\}$. ▮

The following statement follows immediately from Lemma 2.2.8.

Corollary 2.2.9. *Let G be a group, then G is isomorphic to $G \times \{1\} \times \cdots \times \{1\}$, where $\{1\}$ denotes the trivial group.*

Lemma 2.2.8 and Corollary 2.2.9 are quite useful to us. We will use the fact that G is isomorphic to $G \times \{1\} \times \cdots \times \{1\}$ quite often as we go along.

Lemma 2.2.10. *Let G and G' be two groups, and let $H \leq G$ and $H' \leq G'$ be two subgroups. Then $H \times H' \leq G \times G'$.*

Proof: Let G, G' be groups. Let $H \leq G$ and $H' \leq G'$ be two subgroups. Take any element (h, h') of $H \times H'$. Note that $h \in H$ and $h' \in H'$, therefore $(h, h') \in G \times G'$. We can conclude that $H \times H' \subseteq G \times G'$.

Consider two elements (h, h') and $((k)^{-1}, k'^{-1})$ in $H \times H'$ and their product $(h, h')((k)^{-1}, k'^{-1}) = (h(k)^{-1}, h'(k')^{-1})$. Since $h(k)^{-1} \in H$ and $h'(k')^{-1} \in H'$, then $(h(k)^{-1}, h'(k')^{-1}) \in H \times H'$. Therefore $H \times H'$ is a subgroup of $G \times G'$. ∎

Definition 2.2.11. Let G be a group, and let $g_1, \ldots, g_n \in G$. Then $\langle g_1, \ldots, g_n \rangle$ denotes the smallest subgroup of G containing $g_1, \ldots, g_n$.

Lemma 2.2.12. *Let G be a group. Suppose that $a, b, c \in G$ such that $\langle a, b \rangle \leq G$ and $\langle a, c \rangle \leq G$. Then $\langle a, b \rangle = \langle c, a \rangle$ if $ba^i = c$ for some i.*

Proof: By the definition above, $\langle a, b \rangle$ is the smallest subgroup of G that contains a and b but note that both b and a are elements of $\langle c, a \rangle$ since $b = ca^{-i}$. Therefore, $\langle a, b \rangle \subseteq \langle c, a \rangle$.

Similarly, since $\langle c, a \rangle$ is the smallest subgroup of G containing both c and a it must be a subset of any other subgroups containing c and a. Since $c = ba^i$ then $c \in \langle a, b \rangle$ and $\langle c, a \rangle \subseteq \langle a, b \rangle$. ∎

Lemma 2.2.13. *Let G be a group. Let K be a normal subgroup of G. Then K is the kernel of the homomorphism $f : G \to G/K$ defined via $f(g) = gK$.*

Proof: Let G be a group. Let K be a normal subgroup of G.

Let f be the map $f : G \to G/K$ defined via $f(g) = gK$. Note that $f(g_1 g_2) = (g_1 g_2)K = g_1 K g_2 K = f(g_1)f(g_2)$, where the equality $(g_1 g_2)K = g_1 K g_2 K$ comes from the fact that K is normal. Thus, f is a homomorphism. Moreover, f is a surjective map.

Now we will show that K is a kernel of f. Note that for any element $k \in K, k$ is in the kernel of f if and only if $f(k) = K$. Since for any $k \in K$, we have $f(k) = kK = K$, K is the kernel of f. ∎

Now we will introduce a characterization of normal subgroups which is a key to an important theorem which exhibits an important link between homomorphisms and factor groups, the Fundamental Theorem of Group Homomorphisms.

Theorem 2.2.14. *Let G and G' be two groups. Let $f : G \to G'$ be a surjective group homomorphism with kernel K. Then the map $h : G/K \to G'$ defined by $h(gK) = f(g)$ is a group isomorphism.*

Proof: Let G and G' be two groups. Let $f : G \to G'$ be a surjective group homomorphism with kernel K. We will show that the map $h : G/K \to G'$ via $h(gK) = f(g)$ is an isomorphism.

First, note that h is a well-defined map. If $g_1, g_2 \in G$ such $g_1K = g_2K$, then $g_1^{-1}g_2 \in K$, but $K = ker(f)$. Thus, $f(g_1^{-1}g_2) = f(g_1)^{-1}f(g_2)$ is the identity element of G'. Therefore, $f(g_1) = f(g_2)$.

Now, we have shown that if $f(g_1) = f(g_2)$, then $g_1K = g_2K$. Then we can see that $h(g_1K) = h(g_2K)$, implies $g_1K = g_2K$. Moreover, since f is surjective, every element of G' is of the form $f(g)$ for some $g \in G$, thus is of the form $h(gK)$, so h is surjective.

Lastly, we need to show that h is a homomorphism. Since K is normal we have the following equality: $h((g_1)K(g_2)K) = h((g_1g_2)K) = f(g_1g_2) = f(g_1)f(g_2) = h(g_1K)h(g_2K)$. So we can conclude that h is a homomorphism. ∎

We now prove some results about the subgroup structure of groups that will be used in the later sections.

Lemma 2.2.15. *Let G be a group. Let H be a normal subgroup of G. Then there exists a bijection between the set of all subgroups of G containing H and the set of all subgroups of G/H.*

Proof: Let G be a group. Let H be a normal subgroup of G. We will show that there exists a bijection between the set S of all subgroups of G containing H, and the set S' of all subgroups of G/H.

First, let us define a function $f : S \to S'$ by $f(K) = K/H$. Here, K/H is the subset of G/H defined by $K/H = \{kH \mid k \in K\}$. To show the map is well-defined we show K/H is a subgroup of G/H. If $kH, k'H \in K/H$ then $(kH)(k'H)^{-1} = (kH)((k')^{-1}H) = (k(k')^{-1})H$ since H is normal. Since K is a subgroup of G, $k(k')^{-1} \in K$ so $(k(k')^{-1})H \in K/H$. Thus K/H is a subgroup of G/H.

Next, we show f is injective. Suppose $K, K' \in S$ and that $f(K) = f(K')$. Then $K/H = K'/H$. Thus for each $k \in K$, $kH \in K'/H$ so there is some $k' \in K'$ such that $kH = k'H$ or $k \in k'H$. That means there is some $h \in H$ so that $k = k'h$. Since

$H \subseteq K'$, this means $k \in K'$, so $K \subseteq K'$. Exchanging K and K' in this argument shows that $K = K'$.

Finally, we show that f is surjective. Let $\overline{K}$ be a subgroup of G/H. Set $K = \{k \in G \mid kH \in \overline{K}\}$. We show that K is a subgroup of G containing H. If $k, k' \in K$ then $kH, k'H \in \overline{K}$. Since H is normal in G we have $(kH)(k'H)^{-1} = (k(k')^{-1})H$ and since $\overline{K}$ is a subgroup of G/H this product is in $\overline{K}$. Therefore we have $k(k')^{-1} \in K$ and so K is a subgroup of G. Let $h \in H$. Then $hH = H$ which is the identity element of G/H. Therefore $hH \in \overline{K}$ so $h \in K$. Thus $H \subseteq K$ so K is an element of S. Therefore f is surjective.

∎

Suppose G is a cyclic group of prime order p. Then since the order of any element must divide p, every nontrivial element has order p. So G has $\phi(p) = p - 1$ elements of order p. This is a key property we will use several times. For instance consider the following lemma.

Lemma 2.2.16. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. G has $p+1$ non-trivial cyclic subgroups, and each pair of these subgroups intersect only in the identity.*

Proof: The order of the group G is p^2 but because G is not cyclic, it follows that the order of every non-trivial element $g \in G$ is p. If H is a subgroup of G, then $|H| \mid |G|$. So $|H| \in \{1, p, p^2\}$. Since we are looking for the non-trivial cyclic subgroups of G, and G itself is not cyclic, we have that $|H| \neq 1$ and $|H| \neq p^2$. It must be that the order of H is p, and thus H is cyclic.

Notice that there are $p^2 - 1$ elements of order p in the group G. Every cyclic subgroup of order p has $\phi(p) = p - 1$ elements of order p. Now notice that if H and H' are two cyclic subgroups of order p, then their intersection is a subgroup of each, hence either trivial or equal to both of them. It follows that no two distinct cyclic subgroups can have a nontrivial element in common. There are $p-1$ nontrivial elements in each cyclic subgroup, so we have $\frac{p^2-1}{p-1} = p + 1$ subgroups in total. ∎

2.3 Classical query complexity of the Hidden Subgroup Problem for abelian groups

We are now ready to embark on the core of this thesis - algorithms to solve the HSP over various groups. Having a very neat structure and many helpful properties abelian groups are a natural first candidate to consider. In this section we will study the HSP over cyclic groups and direct product of cyclic groups of relatively prime order, as well as the case $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$.

2.3.1 The case of $\mathbb{Z}/p^n\mathbb{Z}$, for a prime p.

As the title suggests we will first study the case $G = \mathbb{Z}/p^n\mathbb{Z}$. Since our goal is to find a hidden subgroup H of G, we must be familiar with the subgroup structure of G. When $G = \mathbb{Z}/p^n\mathbb{Z}$, its subgroups have a very particular architecture, namely they are nested:

$$H_0 = \langle p^{n-0} \rangle \subseteq H_1 = \langle p^{n-1} \rangle \subseteq \cdots \subseteq H_n = \langle p^{n-n} \rangle. \tag{2.3.1}$$

So there are $n + 1$ subgroups of G, and one of these is the hidden subgroup H. Moreover, note that the subgroups of G form a totally ordered set with respect to inclusion. So one might draw similarities between the " $\leq$ " relation in 2.2.6 and the inclusion relation in our case. Keeping these statements in mind, let us begin the theorem.

Theorem 2.3.1. *Let $n \geq 1$. If $G = \mathbb{Z}/p^n\mathbb{Z}$ and H is a hidden subgroup, then it takes an adversary at most $\lceil \log_2(n+1) \rceil + 1$ queries to solve the Hidden Subgroup Problem.*

The idea of the proof is to use the Binary Search Algorithm on the subgroups of G. The goal is to "trap" the subgroup. Every query should split the set of subgroups in two halves, or roughly two halves if $n + 1$ is not a perfect power of two, and determine which of the two sets contains the desired subgroup H. As a result at each consecutive step only a half or roughly a half of the previous set is considered until we arrive at the set containing only one subgroup. That subgroup is H.

Proof: Let $G = \mathbb{Z}/p^n\mathbb{Z}$. Let H be the hidden subgroup in the set of subgroups of G as in the equation 2.3.1. Let f be an H-periodic function hiding H. Then for any g in G,

$$f(0_G) = f(g) \text{ if and only if } g \in H.$$

Suppose that we queried the element p^{n-i}. If $f(p^{n-i}) = f(0_G)$ then $p^{n-i} \in H$. Since all powers of p^{n-i} are also elements of H, thus $H_i \subseteq H$. Now since the subgroups of G are are nested, H must be one of the subgroups $\{H_i, H_{i+1}, \ldots, H_n\}$.

On the other hand, if $f(p^{n-i}) \neq f(0_G)$, then H must be one of the subgroups that do not contain p^{n-i} as an element. Keeping in mind the subgroup structure of G in (2.3.1), such subgroups form the set $\{H_0, \ldots, H_{i-1}\}$. Therefore our binary search algorithm applies.

It is essential to have the value of $f(0_G)$ in order to perform the binary search. Hence, after querying $f(0_G)$ it takes $\lceil \log_2 (n+1) \rceil$ queries to find H in the set of $n+1$ subgroups by Theorem 2.2.6. ∎

We might ask if this attack may be extended to any other class of groups, and the following shows that this is not the case.

Lemma 2.3.2. *The finite abelian groups in which all subgroups are nested are exactly the cyclic groups of order p^k for some prime p.*

Proof: Let G be a cyclic group $G = \langle g \rangle$ of order p^k for some positive integer k. Then every subgroup of G has a form $H = \langle g^{p^{k-l}} \rangle$ for some positive integer l. Thus, subgroups of G are all nested.

We will now show that if a group has order other than p^k or the group is not cyclic or both then not all the subgroups of that group are nested.

Let us consider the first case, namely let $|G'| \neq p^k$. Suppose that the subgroups of G' are nested. Suppose that order of G' is not equal to p^k for any positive k. Then there exist two distinct primes q and r such that $q||G|$ and $r||G|$. Then by [8, Corollary of the Theorem 24.3] G has two subgroups H and K such that $|H| = q$, and $|K| = r$. Since q and r are distinct primes, $H \nsubseteq K$ and $K \nsubseteq H$. Thus the subgroups of G are not nested.

We will now consider the second case. Suppose G' have order p^k, for some positive integer k, but G' is not cyclic. Then $k > 1$. Let h be a generator of a maximal cyclic subgroup H of G' . Since $H \neq G'$, there is some $k \in G'$ which is not contained in H. Thus if $K = \langle k \rangle$, we have $K \not\subset H$. On the other hand, if $H \subseteq K$ then we would have $H = K$ by maximality. So $H \not\subset K$. Therefore the subgroups of G are not nested.

Thus, the only abelian groups with nested subgroups are cyclic groups of prime power order. ∎

2.3.2 The case of general cyclic group $\mathbb{Z}/N\mathbb{Z}$

In this section, we will study the HSP over a general cyclic group $G = \mathbb{Z}/N\mathbb{Z}$. To develop our theory, we begin with a particular example, and derive an algorithm for a base case, before proceeding to the general case.

Consider the case of $N = 675$. Since $675 = 3^3 \times 5^2$, the Chinese Remainder theorem assures us that we have

$$\mathbb{Z}/675\mathbb{Z} \cong \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z}.$$

In fact, we can be explicit. Define a map $\psi\colon \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \to \mathbb{Z}/675\mathbb{Z}$ by setting $\psi([1],[0]) = [3^3]$ and $\psi([0],[1]) = [5^2]$, where $[a]$ means the image of the integer a in the respective group. Since the order of 3^3 in $\mathbb{Z}/675\mathbb{Z}$ is 5^2, and the order of 5^2 in $\mathbb{Z}/675\mathbb{Z}$ is 3^3, this map gives a homomorphism. Conversely, since by the Euclidean algorithm $1 = 13 \times 25 - 12 \times 27$, we deduce that the inverse map ψ^{-1} is generated by sending 1 to $([-12],[13]) = ([13],[13])$. Thus it is an isomorphism. We let π_5 and π_3 denote the projection homomorphisms from $\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z}$ onto each of its direct factors, and ϕ_5 and ϕ_3 the corresponding inclusions.

Next, we note that every subgroup M of $\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z}$ is of the form $E \times K$ with $E \leq \mathbb{Z}/5^2\mathbb{Z}$ and $K \leq \mathbb{Z}/3^3\mathbb{Z}$. By Lemma 2.2.10, each of these is a subgroup of $\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z}$. Suppose $M \leq \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z}$, and let $E = \pi_5(M)$ and $K = \pi_3(M)$. Then these are subgroups of their respective groups, and it is clear that $M \subseteq E \times K$. Because M surjects onto each E and K, their orders must divide the order of M. Since $|E|$ divides 5^2 and $|K|$ divides 3^3, their orders are relatively prime, so $|E \times K| = |E| \times |K|$ necessarily divides $|M|$. Equality follows.

Since $\psi\colon \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \to \mathbb{Z}/675\mathbb{Z}$ is an isomorphism we conclude that every subgroup H of $\mathbb{Z}/675\mathbb{Z}$ is equal to $\psi^{-1}(E \times K)$ for some subgroup E of $\mathbb{Z}/5^2\mathbb{Z}$ and subgroup K of $\mathbb{Z}/3^3\mathbb{Z}$.

However, by Lemma 2.3.2 we know that these subgroups do not form a totally ordered set under inclusion, so the binary search algorithm does not apply. One way to solve this problem is to reduce this direct product to the cyclic case. That is, given a hidden subgroup H of $\mathbb{Z}/675\mathbb{Z}$ such that $\psi^{-1}(H) = E \times K$, we use the binary search algorithm on $\mathbb{Z}/5^2\mathbb{Z}$ to find E, and then the binary search algorithm on $\mathbb{Z}/3^3\mathbb{Z}$ to find K.

Thus the next obstacle is to make sure that any hiding function $f\colon \mathbb{Z}/675\mathbb{Z} \to X$ induces hiding functions for these subgroups E and K. We define

$$f_5\colon \mathbb{Z}/5^2\mathbb{Z} \to X \quad \text{by} \quad f_5(g) = f(\psi(\phi_5(g)))$$

and

$$f_3\colon \mathbb{Z}/3^3\mathbb{Z} \to X \quad \text{by} \quad f_3(g) = f(\psi(\phi_3(g))).$$

Let us show that f_5 is E-periodic; a similar argument works to show that f_3 is K-periodic. So suppose first that $a, b \in \mathbb{Z}$ and $f_5([a]) = f_5([b])$. We have

$$f_5([a]) = f(\psi([a], 0)) = f(\psi(a(1,0)) = f(a\psi(1,0)) = f([3^3 a])$$

and similarly $f_5([b]) = f([3^3 b])$. Since f is H-periodic, this happens if and only if $[3^3 a] - [3^3 b] = [3^3(a-b)] = \psi(([a-b], 0)) \in H$. That is, $f_5([a]) = f_5([b])$ if and only if $[a] - [b] \in E$. Thus f_5 is E-periodic.

This shows us that we have everything that we require to use Theorem 2.3.1.

Our algorithm is as follows:

1. Evaluate $f(0) = f_3(0) = f_5(0)$.

2. Apply Theorem 2.3.1 to the subgroup $\mathbb{Z}/5^2\mathbb{Z}$ and the hiding function f_5 to find the subgroup E in at most log whatever more queries.

3. Apply Theorem 2.3.1 to the subgroup $\mathbb{Z}/3^3\mathbb{Z}$ and the hiding function f_3 to find the subgroup K in at most log whatever steps.

4. The hidden subgroup is $H = \psi(E \times K)$.

Note that for this example to work we required that there exists a homomorphism between $\mathbb{Z}/675\mathbb{Z}$ and $\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z}$, as well as two maps f_5 and f_3 that are $E-$periodic and K-periodic respectively. We will start by generalizing this to all N.

Lemma 2.3.3. *Let H, K, G be groups and let G be abelian. Let $\phi : H \to G$ and $\psi : K \to G$ be group homomorphisms. Then $\phi \times \psi : H \times K \to G$ via $(h, k) \mapsto \phi(h)\psi(k)$ is a group homomorphism.*

Proof: Let H, K, G be groups and let G be abelian. Let $\phi : H \mapsto G$ and $\psi : K \mapsto G$ be group homomorphisms. Define a map $\phi \times \psi : H \times K \mapsto G$ defined via $(h, k) \mapsto \phi(h)\psi(k)$. Then $(\phi \times \psi)(1, 1) = \phi(1)\psi(1) = 1$.

Take two elements (a_H, a_K) and (b_H, b_K) of $H \times K$. Then

$$\begin{aligned}(\phi \times \psi)((a_H, a_K)(b_H, b_K)) &= (\phi \times \psi)(ab_H, ab_K)\\ &= \phi(ab_H)\psi(ab_K) = \phi(a_H)\phi(b_H)\psi(a_K)\psi(b_K)\end{aligned}$$

since ϕ and ψ are group homomorphisms. Since G is abelian

$$\begin{aligned}\phi(a_H)\phi(b_H)\psi(a_K)\psi(b_K) &= \phi(a_H)\psi(a_K)\phi(a_K)\psi(b_K)\\ &= (\phi \times \psi)(a_H, a_K)(\phi \times \psi)(b_H, b_K).\end{aligned}$$

Thus, we can conclude that $\phi \times \psi$ is a homomorphism.

■

Lemma 2.3.4. *Let G_1, G_2 be two groups and $H_1 \leq G_1, H_2 \leq G_2$ be two subgroups. Let X be a finite set. Let $\phi : G_1 \mapsto G_2$ be an injective homomorphism, such that $\phi(H_1) = H_2$. Then $f : G_2 \mapsto X$ is H_2-periodic if and only if $f \circ \phi$ is H_1-periodic.*

Proof: Let G_1, G_2 be two groups and $H_1 \leq G_1, H_2 \leq G_2$ be two subgroups. Let X be a finite set. Let $\phi : G_1 \mapsto G_2$ be an injective homomorphism, such that $\phi(H_1) = H_2$. Suppose that $f : G_2 \mapsto X$ is H_2-periodic. We want to show that

$$f \circ \phi(a) = f \circ \phi(b) \text{ if and only if } aH_1 = bH_1 \text{ for any } a, b \in G_1.$$

Suppose that $f \circ \phi(a) = f \circ \phi(b)$ then $f(\phi(a)) = f(\phi(b))$ and since f is H_2-periodic $\phi(a)H_2 = \phi(b)H_2$. This implies that $\phi(a)(\phi(b))^{-1} \in H_2$ and since ϕ is a homomorphism $\phi(ab^{-1}) \in H_2$. Since ϕ is injective, $ab^{-1} \in H_1$.

Suppose that $a + H_1 = b + H_1$ so that $ab^{-1} \in H_1$. After applying ϕ to (ab^{-1}) and H_1, since ϕ is a homomorphism we get $\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1} \in H_2$. Thus, $\phi(a)H_2 = \phi(b)H_2$, implying that $f \circ \phi(a) = f \circ \phi(b)$.

Now suppose that $f \circ \phi(a)$ is H_1-periodic. We want to show that

$$f(c) = f(d) \text{ if and only if } cH_2 = dH_2 \text{ for any } c, d \in G_2.$$

Notice that $H_2 = \phi(H_1)$, thus the statement becomes

$$f(\phi(a)) = f(\phi(b)) \text{ if and only if } \phi(a)H_2 = \phi(b)H_2 \text{ for any } a, b \in H_1.$$

Suppose that $f \circ \phi(a) = f \circ \phi(b)$, then since $f \circ \phi$ is H_1-periodic we get $aH_1 = bH_1$. Applying ϕ to both sides of the equation results in $\phi(a)\phi(H_1) = \phi(b)\phi(H_1)$, so $\phi(a)H_2 = \phi(b)H_2$.

Suppose that $\phi(a)H_2 = \phi(b)H_2$. Since ϕ is injective, $aH_1 = bH_1$. So we have $f \circ \phi(a) = f \circ \phi(b)$. ∎

Now that we have stated and proven Lemma 2.3.3 and Lemma 2.3.4, we can move on to the result stating the complexity of solving the HSP over $G = \mathbb{Z}/N\mathbb{Z}$, where N is a product of two prime powers.

Theorem 2.3.5. *Let $n, m \geq 1$ be two positive integers. Let p, q be two distinct primes. Given $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/q^m\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$ where $N = p^n q^m$, it takes at most $\lceil \log_2(m+1) \rceil + \lceil \log_2(n+1) \rceil + 1$ queries to find the hidden subgroup H.*

Proof: Let $n, m \geq 1$ be two positive integers. Let p, q be two positive primes such that $\gcd(p, q) = 1$. Let $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/q^m\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}$ where $N = p^n q^m$. Consider subgroups of $\mathbb{Z}/N\mathbb{Z}$. Any subgroup of $\mathbb{Z}/N\mathbb{Z}$ is isomorphic to $E_i \times K_j = \langle p^{n-i} \rangle \times \langle q^{m-j} \rangle$, for $i \in \{0, \ldots, n\}$ and $j \in \{0, \ldots, m\}$. In particular, we may assume our hidden subgroup is $H \cong E \times K$.

Let ϕ_p be the injection of $\mathbb{Z}/p^n\mathbb{Z}$ into $\mathbb{Z}/N\mathbb{Z}$ and set $f_p(x) = f(\phi_p(x))$, and let ψ_q be the injection of $\mathbb{Z}/q^m\mathbb{Z}$ into $\mathbb{Z}/N\mathbb{Z}$ and set $f_q(y) = f(\psi_q(y))$.

Let $f_p : \mathbb{Z}/p^n\mathbb{Z} \mapsto X$ be the function defined above, then f_p is E-periodic. Hence, such function allows us to query elements of $\mathbb{Z}/p^n\mathbb{Z}$, and in particular, generators of the subgroups E_i. By the Theorem 2.3.1 we can use binary search algorithm on $\mathbb{Z}/p^n\mathbb{Z}$ to find E, once we know the value $f_p(0) = f(0)$. Similarly a function $f_q : \mathbb{Z}/q^m\mathbb{Z} \mapsto X$ defined above is K-periodic. This allows us to query elements of $\mathbb{Z}/q^m\mathbb{Z}$ and by the Theorem 2.3.1 we can use the binary search to find K, once we know $f_q(0) = f(0)$. As a result we can construct H since $\psi(E \times K) = H$.

Note that $\mathbb{Z}/p^n\mathbb{Z}$ has $n+1$ subgroups and $\mathbb{Z}/q^m\mathbb{Z}$ has $m+1$ subgroups. Hence, by the Theorem 2.2.6 above it will take at most $\lceil \log_2 (n+1) \rceil$ queries to find E and at most $\lceil \log_2 (m+1) \rceil$ queries to find K, once the identity element has been queried. Both of the groups are cyclic, thus it suffices to query the identity element once. Thus, in total it takes at most $\lceil \log_2 (m+1) \rceil + \lceil \log_2 (n+1) \rceil + 1$ queries. ∎

Ideally, we would like to extend this result to when N is not just a product of two prime powers, but N is any composite number with known factorization. The following lemmas will help us arrive at our final argument of this sections, stating the complexity to solve the HSP over $\mathbb{Z}/N\mathbb{Z}$, where N is any composite number.

First, we show that the result of Lemma 2.3.3 can be extended to any number of factors.

Let k be a positive integer. Let $H_1, \ldots, H_k$ and G be groups and let G be abelian. Let $\phi_i : H_i \to G$ be group homomorphisms, for any $i \in \{1, \ldots, k\}$. Then $\phi_i \times \cdots \times \phi_k : H_1 \times \cdots \times H_k \to G$ via $(h_1, \ldots, h_k) \mapsto \phi_1(h_1) \cdots \phi_k(h_k)$ is also a group homomorphism.

Lemma 2.3.6. *For any set of distinct prime numbers $\{p_1, \ldots, p_k\}$ and positive integers $\{e_1, \ldots, e_k\}$ set $N = \prod_{i=1}^{k} {p_i}^{e_i}$. Then the map $\theta : \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z} \mapsto \mathbb{Z}/N\mathbb{Z}$ defined on generators by*

$$\begin{aligned} (1, 0, \ldots, 0) &\mapsto {p_2}^{e_2}{p_3}^{e_3} \ldots {p_k}^{e_k} \\ (0, 1, \ldots, 0) &\mapsto {p_1}^{e_1}{p_3}^{e_3} \ldots {p_k}^{e_k} \\ &\vdots \\ (0, 0, \ldots, 1) &\mapsto {p_1}^{e_1}{p_2}^{e_2} \ldots {p_{k-1}}^{e_{k-1}} \end{aligned} \tag{2.3.2}$$

is an isomorphism.

Proof: Let $\{p_1, \ldots, p_k\}$ be a set of distinct prime numbers and $\{e_1, \ldots, e_k\}$ be a set of positive integers and set $n = \prod_{i=1}^{k} {p_i}^{e_i}$. Note that $\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ and $\mathbb{Z}/N\mathbb{Z}$ are groups and $\prod_{j \neq i} p_j^{e_j}$ is a nonzero element of $\mathbb{Z}/N\mathbb{Z}$. Since $\prod_{j \neq i} p_j^{e_j}$ is a positive divisor of N, then the order of $\prod_{j \neq i} p_j^{e_j}$ in $\mathbb{Z}/N\mathbb{Z}$ is $\frac{n}{\prod_{j \neq i} p_j^{e_j}} = {p_i}^{e_i}$. It follows that there exists an injective homomorphism

$$\theta_i : \mathbb{Z}/{p_i}^{e_i}\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \text{ such that } 1 \mapsto \prod_{j \neq i} p_j^{e_j}. \tag{2.3.3}$$

Let $H_i = \langle \prod_{j \neq i} p_j^{e_j} \rangle$. Then $\theta_i(\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}) = H_i$. So by Lemma 2.3.3, since our map θ is just the product of the maps θ_i, it is a homomorphism

$$\theta : \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z} \mapsto \mathbb{Z}/N\mathbb{Z}$$

with image

$$\theta(\mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}) = H_1 \times \cdots \times H_k.$$

We will now prove that θ is an injective homomorphism. Notice that

$$\ker(\theta) = \{([a_1], [a_2], \ldots, [a_k]) : [a_i] \in \mathbb{Z}/{p_i}^{e_i}\mathbb{Z},\ \theta([a_1], [a_2], \ldots, [a_k]) = 0\} \tag{2.3.4}$$

So $a_1 \prod_{j \neq 1} p_j^{e_j} + \cdots + a_k \prod_{j \neq k} p_j^{e_j} = 0$ in $\mathbb{Z}/N\mathbb{Z}$, for a_i being a representative of $[a_i]$, for $i \in \{1, \ldots, k\}$. Reducing the equality modulo ${p_i}^{e_i}$ for every $i \in \{1, \ldots . k\}$ results in $a_1 = a_2 = \cdots = a_k = 0$. Therefore, θ is an injective homomorphism.

Note that the cardinality of $\mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}$ is equal to the cardinality of $\mathbb{Z}/N\mathbb{Z}$.Therefore the map θ is surjective.

So $\theta : \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z} \mapsto \mathbb{Z}/N\mathbb{Z}$ is an isomorphism.

Consider now any subgroup $\langle {p_1}^{d_1}\rangle \times \langle {p_2}^{d_2}\rangle \times \cdots \times \langle {p_k}^{d_k}\rangle$ of $\mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}$. Then since $\gcd({p_1}^{e_1-d_1} + \cdots + {p_k}^{e_k-d_k}, n) = 1$,

$$\begin{aligned}\theta(\langle {p_1}^{d_1}\rangle \times \langle {p_2}^{d_2}\rangle \times \cdots \times \langle {p_k}^{d_k}\rangle) &= \theta(\langle {p_1}^{d_1}, \ldots, {p_k}^{d_k}\rangle) \\ &= \langle \theta({p_1}^{d_1}, \ldots, {p_k}^{d_k})\rangle = \langle {p_1}^{d_1} \cdots {p_k}^{d_k}({p_1}^{e_1-d_1} + \cdots + {p_k}^{e_k-d_k})\rangle \qquad (2.3.5) \\ &= \langle {p_1}^{d_1} \cdots {p_k}^{d_k}\rangle.\end{aligned}$$

∎

From the above lemma we can derive that $\theta(0, \ldots, 0, [a], 0, \ldots, 0) = a \prod_{j \neq i} p_j^{e_j}$ for any $a \in \mathbb{Z}$ representing $[a] \in \mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$.

Lemma 2.3.7. *For any set of distinct prime numbers $\{p_1, \ldots, p_k\}$ and positive integers $\{e_1, \ldots, e_k\}$ set $N = \prod_{i=1}^{k} {p_i}^{e_i}$. Let θ be the isomorphism defined in Lemma 2.3.6. Then for any $H \leq \mathbb{Z}/N\mathbb{Z}$ there exist subgroups $E_i \leq \mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ for every $i \in \{1, \ldots, k\}$, such that $\theta^{-1}(H) = E_1 \times \cdots \times E_k$.*

Proof: For any set of distinct prime numbers $\{p_1, \ldots, p_k\}$ and positive integers $\{e_1, \ldots, e_k\}$ set $N = \prod_{i=1}^{k} {p_i}^{e_i}$. Let θ be the isomorphism defined in Lemma 2.3.6. Take any $H \leq \mathbb{Z}/N\mathbb{Z}$. Set

$$G = \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}.$$

Note that for any $i \in \{1, \ldots, k\}$, $|\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}| = {p_i}^{e_i}$ and $|G| = {p_1}^{e_1} \ldots {p_k}^{e_k}$.

Let $E = \theta^{-1}(H) \leq G$. Then $|E| \mid {p_1}^{e_1} \ldots {p_k}^{e_k}$. This means that $|E| = {p_1}^{d_1} \ldots {p_k}^{d_k}$ where $d_i \mid e_i$ for every $i \in \{1, \ldots, k\}$.

Let $\pi_i : G \mapsto \mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ be the projection for all $i \in \{1, \ldots, k\}$. Let $\pi_i(E) = E_i$ for all $i \in \{1, \ldots, k\}$ so that $E_i \leq \mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$. Since E_i is a homomorphic image of E, we have $|E_i| \mid |E|$. Therefore, $|E_i| = {p_i}^{k_i}$ for some $k_i \leq e_i$.

Note that

$$E \subseteq E_1 \times \cdots \times E_k, \text{ thus } |E| \mid |E_1 \times \cdots \times E_k|.$$

It follows that $|E_1 \times \cdots E_k| \leq |E|$ and $|E| \leq |E_1 \times \cdots E_k|$, so the orders equal. Therefore, $E = E_1 \times \cdots \times E_k$. ∎

Let $N = \prod_{i=1}^{k} {p_i}^{e_i}$, for any set of distinct prime numbers $\{p_1, \ldots, p_k\}$ and positive integers $\{e_1, \ldots, e_k\}$. Let θ_i be the map defined in the equation (2.3.3). Let $H \leq$

$\mathbb{Z}/N\mathbb{Z}$. By Lemma 2.3.7, $H = \theta^{-1}(E_1 \times \cdots \times E_k)$, where $E_i \leq \mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ for each $i \in \{1, \ldots, k\}$. If $f : \mathbb{Z}/N\mathbb{Z} \mapsto X$ is a H-periodic function, then

$$f_i(a) = f(\theta_i(a)) = f(a \prod_{j \neq i} p_j^{e_j})$$

is E_i-periodic for any $i \in \{1, \ldots, k\}$.

Now we finally arrived at the theorem stating complexity of the HSP over $\mathbb{Z}/N\mathbb{Z}$, where N is any composite number.

Theorem 2.3.8. *Suppose $N > 1 \in \mathbb{N}$ has prime factorization $N = \prod_{i=1}^{k} p_i^{e_i}$ such that $gcd(p_1, \ldots, p_k) = 1$ and $\{e_1, \ldots, e_k\}$ are positive integers. Then it takes at most $\lceil \log_2 (e_1 + 1) \rceil + \cdots + \lceil \log_2 (e_k + 1) \rceil + 1$ queries to find the hidden subgroup H of $\mathbb{Z}/N\mathbb{Z}$.*

Proof: Let $H \leq \mathbb{Z}/N\mathbb{Z}$. By Lemma 2.3.7 $H \cong E_1 \times \cdots \times E_k$, where each $E_i \leq \mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$, for all $i \in \{1, \ldots, k\}$. Let $f_i : \mathbb{Z}/{p_i}^{e_i}\mathbb{Z} \mapsto X$ be the E_i-periodic function defined in Lemma 2.3.4. By Lemma 2.3.1 we can find E_i in at most $\lceil \log_2 (e_i + 1) \rceil$ steps, once we know the value $f(0)$. Since each E_i is a cyclic subgroup, it suffices to query the identity element once. As a result we can construct H since $\theta(E_1 \times \cdots \times E_k) = H$. In total, that makes $\lceil \log_2 (e_1 + 1) \rceil + \cdots + \lceil \log_2 (e_k + 1) \rceil + 1$ queries. ∎

Now that we know the complexity of the HSP over a general abelian group, it is desirable to go back to the Theorem 2.1.2. Recall, that Theorem 2.1.2 states that if the group G has a set of k nontrivial subgroups whose only common element is the identity, then in the worst case the number of queries a classical computer must make to solve HSP is at least $\sqrt{2k}$. The following lemma will help us compare the result of the theorem 2.1.2 to 2.3.8 in the case of an abelian group $\mathbb{Z}/N\mathbb{Z}$ for any N.

Lemma 2.3.9. *Suppose $N > 1 \in \mathbb{N}$ has prime factorization $N = \prod_{i=1}^{k} p_i^{e_i}$ such that $p_1, \ldots, p_k$ are distinct primes and $\{e_1, \ldots, e_k\}$ are positive integers. Then the maximum number of nontrivial subgroups of $\mathbb{Z}/N\mathbb{Z}$ that intersect trivially is k.*

Proof: By Lemma 2.3.7 it suffices to consider subgroups of $\mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}$. Note that

$$E_1 \times \cdots \times E_k \cap F_1 \times \cdots \times F_k = E_1 \cap F_1 \times \cdots \times E_k \cap F_k.$$

Thus, this intersection is trivial if and only if

$$E_i \cap F_i = \{0\}, \text{ for all } i \in \{1, \ldots, k\}.$$

So it suffices to consider pairwise intersections of subgroups of the form $E_i \cap F_i$, where each E_i and F_i are subgroups of $\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ for any $i \in \{1, \dots, k\}$ and $E_i \cap F_i = \{0\}$. Since for each $i \in \{1, \dots, k\}$ subgroups of each $\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ are nested, the intersection $E_i \cap F_i$ is trivial if and only if one of E_i or F_i is trivial.

More precisely, if subgroups of $\mathbb{Z}/{p_i}^{e_i}\mathbb{Z}$ are $\{\{0\}, \langle p_1\rangle, \langle {p_1}^{d_1}\rangle, \langle {p_2}^{d_2}\rangle, \dots, \langle {p_k}^{d_k}\rangle\}$, then by Lemma 2.3.6 we would like E_i or F_i be a subgroup $\langle {p_1}^{d_i}\rangle$ for exactly one $i \in \{1, \dots, k\}$, and the rest of the subgroups to be trivial. So the subgroups that intersect trivially look like

$$\langle 0\rangle \times \cdots \times \langle {p_1}^{d_i}\rangle \times \cdots \times \langle 0\rangle \text{ and } \langle 0\rangle \times \cdots \times \langle {p_1}^{d_j}\rangle \times \cdots \times \langle 0\rangle.$$

It follows that $\mathbb{Z}/N\mathbb{Z}$ has k subgroups that intersect trivially. ∎

So if the group we are working with is $G = \mathbb{Z}/{p_1}^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_k}^{e_k}\mathbb{Z}$, it takes at least $\sqrt{2k}$ and at most $\lceil \log_2{(e_1+1)}\rceil + \cdots + \lceil \log_2{(e_k+1)}\rceil + 1$ queries to find the Hidden Subgroup. To compare the two bounds note that we are allowed to take k as large as we want, however, we require $e_1, \dots, e_k$ to be positive integers. Thus, the supremum of the number of the queries it takes at most to find the hidden subgroup problem is $\lceil \log_2{(1+1)}\rceil + \cdots + \lceil \log_2{(1+1)}\rceil + 1 = k+1$.

2.3.3 The case of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, for a prime p.

We are now going to explore the structure theory of noncyclic abelian groups. In this section we will use additive notation solely. We will start off with a remarkable observation that makes it possible to design an attack to solve the HSP over $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Lemma 2.3.10. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. For any cyclic subgroup $H \leq G$ and any $g \in G \setminus H$, the coset $g + H$ has exactly one element of every other cyclic subgroup $K \leq G$.*

Proof: Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Let H be a non-trivial cyclic subgroup of G. Suppose to the contrary that the coset $g + H$ contains two distinct elements $k_1 = g + h_1$ and $k_2 = g + h_2$ of the same non-trivial cyclic subgroup K.

Since $k_1 - k_2 \in K$, and $k_1 - k_2 = h_1 - h_2$, the element of the subgroup K is also an element of H. That would imply a contradiction by Lemma 2.2.16. So it must be that $k_1 = k_2$.

Now we will show using a counting argument that there is an element of each non-trivial cyclic subgroup except for H, in $g + H$. By Lemma 2.2.16, there are $p+1$ non-trivial cyclic subgroups, each having p elements. Thus, the coset $g+H$ has p elements, and there are p non-trivial subgroups other than H. Since $g+H$ can only have one element from each of the non-trivial cyclic subgroups other than H, we conclude that $g+H$ has exactly one element of each non-trivial cyclic subgroup other than H. ∎

Another interesting consequence of Lemma 2.2.16 is that the maximal number of non-trivial subgroups of $G = \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ that intersect trivially pairwise is $p+1$. That is true because the subgroups of $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ are either cyclic of order p, or trivial subgroup and the entire group G. There are $p+1$ cyclic subgroups of order p in G. Any two of this subgroups intersect trivially. The entire group does not intersect trivially with any of the cyclic subgroups of order p.

Now that we saw the relations between elements of each coset of the non-trivial cyclic subgroups of $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$, we would like to see how the cosets themselves are related.

Lemma 2.3.11. *Let G be a group. Let H be a subgroup. Let $g_i, g_j \in G$. Then $g_i+H = g_j+H$ if and only if $g_i-g_j \in H$. In particular, $g_i+\langle g_i-g_j\rangle = g_j+\langle g_i-g_j\rangle$.*

Recall, that given a function f hiding H it is true that $f(g) = f(g')$ if and only if $g-g' \in H$. When we are dealing with subgroups of $G = \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$, by Lemma 2.2.16 if any $g \neq g'$ is such that $g-g' \in H$, then $H = \langle g-g'\rangle$. We would usually compare $f(g)$, for any $g \in G$ to $f(0)$ in order to find H. Perhaps, it is wise to change our strategy and compare elements to each other in order to find g, g' such that $H = \langle g-g'\rangle$. The subgroups of $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ are not nested so simply comparing elements to each other will not be a particularly smart strategy. Let us see if we can introduce certain conditions on the elements that we query to improve the complexity of the algorithm. Our first attempt is the following.

Theorem 2.3.12. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. Suppose that the hidden subgroup is a nontrivial cyclic subgroup $H \leq G$. It takes $\mathcal{O}(\lceil\frac{p+1}{2}\rceil)$ queries to find H.*

Proof:

Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. Suppose H is a nontrivial cyclic subgroup of G hidden by the function $f\colon G \to X$. Note that for any $g \neq g' \in G$, if $f(g) = f(g')$ then $g-g'$ is a nontrivial element of H, and is therefore a generator. Thus it suffices to find two distinct elements of G that map to the same element of X under f.

Our algorithm to find H is as follows. Set $g_0 = e$ and let $g_1 \in G$ be chosen at random. We query $f(g_0)$ and $f(g_1)$; if they are equal we are done; otherwise, we store the pairs $(g_i, f(g_i))$ for $i = 0, 1$. We define $\mathcal{S}_1 = \{\langle g_1\rangle\}$ to be the set of subgroups that we have so far eliminated as candidates for H.

At the ith step, we choose $g_i \in G$ so that neither g_i, nor g_i-g_1 lies in any subgroup in $\mathcal{S}_{i-1}$. If $f(g_i)$ agrees with a previously computed value, then we have found H; otherwise, let

$$\mathcal{S}_i = \mathcal{S}_{i-1} \cup \{\langle g_i-g_j\rangle \mid 0 \leq j < i\}.$$

The hypothesis on g_i ensures that $|\mathcal{S}_i| \geq |\mathcal{S}_{i-1}| + 2$.

The algorithm terminates when either H is found, or when no such g_i can be found. We claim that this latter case happens only when we have eliminated all subgroups except one.

Note that $g_i - g_1$ is in a subgroup $K \in \mathcal{S}_{i-1}$ if and only if $g_i \in g_1 + K$. So at step i we must choose g_i in the complement of the sets

$$S = \bigcup_{K \in \mathcal{S}_{i-1}} K \quad \text{and} \quad g_1 + S = \bigcup_{K \in \mathcal{S}_{i-1}} (g_1 + K).$$

Let us show this complement is nonempty. We have

$$|S \cup (g_1 + S)| = |S| + |g_1 + S| - |S \cap (g_1 + S)|.$$

We have $|S| = |g_1 + S|$.

Suppose there are $k+1$ subgroups in $\mathcal{S}_{i-1}$ and we have not yet found H. Therefore $k + 1 < p + 1$ or $k < p$ since there are $p + 1$ cyclic subgroups in G. The first subgroup is $\langle g_1 \rangle$, of order p, which meets all others in exactly the identity element. Therefore

$$|S| = p + k(p - 1).$$

Note that $\langle g_1 \rangle \subset S \cap (g_1 + S)$. By Lemma 2.4.7, each of the k remaining subgroups $K \in \mathcal{S}_{i-1}$ meet each coset $g_1 + K'$, for $K \neq K'$, in exactly one element $h_{K,K'}$. If $K' = \langle g_1 \rangle$, then $h_{K,K'} = e \in \langle g_1 \rangle$; otherwise, $h_{K,K'} \notin \langle g_1 \rangle$ and is distinct from all others. Therefore we have

$$|S \cap (g_1 + S)| = |\langle g_1 \rangle| + |\{h_{K,K'} \mid K \neq K', K \neq \langle g_1 \rangle, K' \neq \langle g_1 \rangle\}| = p + k(k - 1).$$

Thus we have

$$|S \cup (g_1 + S)| = 2(p + k(p-1)) - (p + k(k-1)) = p + 2k(p-1) - k(k-1) = p + (2p - k - 1)k.$$

The maximum value of the function $p + (2p - k - 1)k$, as a function of k, is attained at $k = p - \frac{1}{2}$. As k is an integer and $k < p$ the maximum value of $|S \cup (g_1 + S)|$ is $p + (2p - (p - 1) - 1)(p - 1) = p^2 = |G|$, attained when $k = p - 1$. That is, the complement of this set is nonempty (and therefore we cannot choose g_i) only if we have eliminated all but one subgroup in step $i - 1$ — in which case this remaining subgroup must be H, and we are done.

Since at step 1 we eliminate 1 subgroup and at each further step i, we eliminate at least two subgroups, we have

$$|\mathcal{S}_i| \geq 2i - 1.$$

Therefore in the worst case this algorithm terminates in when $2i - 1 = p$. ∎

In this proof, we "eliminated" only two subgroups at each step because we effectively only compared our query $f(g_i)$ with $f(g_0)$ and $f(g_1)$. One might wonder whether it is possible to compare queried elements to more than two elements. Perhaps by comparing more elements we will be able to "eliminate" more subgroups at each step. Now wouldn't that be wonderful! Lemma 2.1.3 tells us that if we query elements of G in a particular fashion that would allow us to "eliminate" $\frac{n(n+1)}{2}$ subgroups by the n-th query. This is much better than the result of the Theorem 2.3.12. Let us call this strategy optimal, in the sense that it yields an attack of optimal complexity $O(\sqrt{p})$.

Unfortunately, the following example shows that there is a subtlety which makes it impossible to choose all queried elements that would maximize the number of "eliminated" subgroups.

Example. Let $G = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. The group G has 8 cyclic subgroups:

$$H_1 = \langle (1,0) \rangle = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(6,0)\}$$

$$H_2 = \langle (0,1) \rangle = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(0,6)\}$$

$$H_3 = \langle (1,1) \rangle = \{(0,0),(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)\}$$

$$H_4 = \langle (1,2) \rangle = \{(0,0),(1,2),(2,4),(3,6),(4,1),(5,3),(6,5)\}$$

$$H_5 = \langle (1,3) \rangle = \{(0,0),(1,3),(2,6),(3,2),(4,5),(5,1),(6,4)\}$$

$$H_6 = \langle (1,4) \rangle = \{(0,0),(1,4),(2,1),(3,5),(4,2),(5,6),(6,3)\}$$

$$H_7 = \langle (1,5) \rangle = \{(0,0),(1,5),(2,3),(3,1),(4,6),(5,4),(6,2)\}$$

$$H_8 = \langle (1,6) \rangle = \{(0,0),(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}$$

We would like to maximize the number of subgroups "eliminated" at each step. If we follow Lemma 2.1.3, then at the i-th query we can eliminate $l = \frac{i(i+1)}{2}$ subgroups. So our steps are as follows.

Step 0: Query $g_0 = (0,0)$

Step 1: Query $g_1 = (1,0)$. Suppose $f(g_0) \neq f(g_1)$, then $H \neq H_1$. We eliminated H_1 and continue our attack.

Step 2: Query an element $g_2 \notin g_l + \langle g_k - g_j \rangle$ for all $0 \leq j,k,l < 2$. In this case this condition is just $g_2 \notin H_1$, so we can pick $g_2 = (0,1)$.

Suppose that $f(g_0) \neq f(g_2)$, then $H \neq H_2$. Suppose also that $f(g_1) \neq f(g_2)$, then $H \neq \langle g_2 - g_1 \rangle = \langle (6,1) \rangle = H_8$. We eliminated H_2, H_8 and we continue the attack.

Step 3: Query an element $g_3 \notin g_l + \langle g_k - g_j \rangle$ for all $0 \leq j, k, l < 3$. After making a table of values, we see that we can pick $g_3 = (2, 2)$.

Suppose that $f(g_0) \neq f(g_3)$, then $H \neq H_3$. Suppose also that $f(g_1) \neq f(g_3)$, then $H \neq \langle (g_3) - (g_1) \rangle = \langle (1, 2) \rangle = H_4$. And finally, suppose that $f(g_2) \neq f(g_3)$, then $H \neq \langle (g_3) - (g_2) \rangle = \langle (2, 1) \rangle = H_6$. We eliminated H_3, H_4, H_6.

Step 4: Query any element $g_4 \notin g_l + \langle g_k - g_j \rangle$ for all $0 \leq j, k, l < 4$. Notice that this set is empty so we are not able to pick g_4 in this fashion.

We have eliminated 6 subgroups out of 8 so there are still subgroups yet to be eliminated. However, we can no longer query elements according to Lemma 1.1.3, to maximize the number of subgroups "eliminated" at every query.

Let us investigate this phenomenon a little more. For example, one question we would like answered is whether at the j-th step, for a certain j, we can still query elements in the same fashion as Lemma 2.1.3, and whether there are still subgroups left to check.

Suppose we are in the following set up. Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Suppose H is the hidden subgroup. For all $i \in \{0, \ldots, p+1\}$, let $K_i = \langle k_i \rangle$ be cyclic subgroups of G.

Let g_0 be the identity element. We will now find a lower bound on the total number of queries it takes to find H. We will use Theorem 2.1.3 and 2.3.12 to obtain this bound. Suppose that the technique of Lemma 2.1.3 is optimal. Then, begin by querying elements starting with g_0, such that at every query j, the queried elements $g_j \notin g_k + \langle g_s - g_t \rangle$, for all $0 \leq k, s, t < j$.

Note that if at any step $f(g_k) = f(g_t)$, then $g_k - g_t \in H$. So if at any step none of the queries are equal, it still remains to find the hidden subgroup H.

The algorithm to solve the HSP over $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is as follows.

Algorithm 2.3.13. Let p be a prime. Here is an algorithm to solve the HSP over $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. For every query g_i, let S_i be the set of all subgroups generated by combinations of the form $g_k - g_l$, where g_k, g_l are queried elements for all $k, l \in \{0, \ldots, i\}$.

First query the identity element $g_0 = e$. For the subsequent queries, query elements g_i such that $g_i \notin g_k + \langle g_s - g_t \rangle$, for all $0 \leq k, s, t < i$.

If at any step $f(g_i) = f(g_k)$, then $H = \langle g_i - g_k \rangle$, so we win. If none of the queries are equal to each other, we continue querying elements in the same fashion.

If we successfully performed j queries but can not query g_{j+1} such that $g_{j+1} \notin g_k + \langle g_s - g_t \rangle$, for all $0 \leq k, s, t < j+1$, then we stop and change our technique.

Starting from the $j+1$-st query, we query elements g_v such that $\langle g_v - g_1 \rangle \notin S$, and $\langle g_v \rangle \notin S$. If at any step $f(g_i) = f(g_k)$, then $H = \langle g_i - g_k \rangle$, so we win.

If none of the queries are equal, continue in this fashion until all cyclic subgroups of G are "eliminated" from the list of possibilities for H. Then H is a trivial subgroup.

It is not a trivial problem to calculate exactly at which step j we can no longer find an element g_j satisfying the hypotheses of Lemma 2.1.3. However by Lemma 2.1.3, we know that having more subgroups left to check means that $l = \frac{1}{2}j(j+1) < p+1$, or that $j < \frac{1}{2}(-1+\sqrt{8p+9})$. We are able to prove the following result.

Lemma 2.3.14. *Suppose $p > 15$. In algorithm 2.3.13 we can perform at least $j = \lfloor p^{\frac{1}{3}} \rfloor$ queries in the same fashion as the Lemma 2.1.3.*

Proof: Let $S_2 = \{g_0, g_1, \ldots, g_j\}$ be a set of elements satisfying the hypotheses of Lemma 2.1.3. Let $\mathcal{S}_1$ be the resulting set of subgroups of G, that is, the set of all subgroups of the form $\langle g_i - g_t \rangle$ for $0 \le i < t \le j$. Note that $|\mathcal{S}_1| = l = \frac{1}{2}j(j+1)$. Let S_3 be the set of all elements of G that lie in a subgroup in $\mathcal{S}_1$, or a coset of such a subgroup by another element of S_2. Our algorithm for finding H using the argument of Lemma 2.1.3 stops when $S_3 = G$, that is when we cannot find an element g_{j+1} outside of all of these cosets.

Let

$$T = \bigcup_{K \in \mathcal{S}_1} K$$

and for each $t \in \{1, \ldots, j\}$ let

$$R_t = \bigcup_{K \in \mathcal{S}_1, K \neq \langle g_t \rangle} (g_t + K).$$

Then $|T| = l(p-1)+1$ since there are l cyclic subgroups of order p, all with only the identity in common. We similarly have $|R_t| = (l-1)(p-1)+1$. We now estimate their intersection.

Note that $T \cap R_t = \bigcup_{K,L \in \mathcal{S}_1, L \neq \langle g_1 \rangle} (g_t + L) \cap K$. Suppose now that $K \in \mathcal{S}_1$ and $L \in \mathcal{S}_1 \setminus \{\langle g_t \rangle\}$. Then

$$(g_t + L) \cap K = \begin{cases} \emptyset & \text{if } K = L, \\ \{g_t\} & \text{if } K = \langle g_t \rangle, \\ \{h_{t,L,K}\} & \text{if } K \neq L,\ K \neq \langle g_t \rangle \end{cases}$$

where these elements $h_{t,L,K}$ are distinct. Therefore for each t we have $|R_t \cap T| = 1 + (l-1)(l-2)$.

Now we note that

$$|S_3| = |T \cup R_1 \cup \ldots R_j| \le |T| + \sum_{t=1}^{j} |R_t| - \sum_{t=1}^{j} |R_t \cap T|.$$

We have

$$|R_t| - |R_t \cap T| = (l-1)(p-1) + 1 - (1 + (l-1)(l-2)) = (l-1)(p-l+1).$$

Therefore we may estimate

$$|S_3| \leq l(p-1) + 1 + j(l-1)(p-l+1).$$

Since $1-l<0$, $l-1<l$, and $p-l+1<p$ we have that

$$|S_3| < lp + jlp = (j+1)lp.$$

Now if $j = \lfloor p^{\frac{1}{3}} \rfloor$, then $j < p^{\frac{1}{3}}$. Using this inequality, we get that if $j = \lfloor p^{\frac{1}{3}} \rfloor$, then

$$\begin{aligned}|S_3| &< (p^{\frac{1}{3}}+1)(\frac{1}{2}p^{\frac{1}{3}}(p^{\frac{1}{3}}+1))p \\ &= \frac{1}{2}p^{\frac{4}{3}}(p^{\frac{1}{3}}+1) \\ &= \frac{1}{2}p^2 + p^{\frac{5}{3}} + \frac{1}{2}p^{\frac{4}{3}}\end{aligned}$$

Our goal now is to show whether it is possible to have $|S_3| < p^2$, when $j = \lfloor p^{\frac{1}{3}} \rfloor$. Note that $p^{\frac{5}{3}} + \frac{1}{2}p^{\frac{4}{3}} < \frac{1}{2}p^2$ if and only if $p^{\frac{1}{3}} + \frac{1}{2} < \frac{1}{2}p^{\frac{2}{3}}$. Letting $p^{\frac{1}{3}} = x$, and solving quadratic inequality $x + \frac{1}{2} < \frac{1}{2}x^2$ yields two roots, namely $x = 1+\sqrt{2}$, and $x = 1-\sqrt{2}$. Since $p \geq 2$, $x = 1+\sqrt{2}$ is the only valid root. This yields $p^{\frac{1}{3}} > 1+\sqrt{2}$, which in turn implies $p > (1+\sqrt{2})^3 > 14$.

So if $p \geq 15$ and $j = \lceil p^{\frac{1}{3}} \rceil$, then

$$|S_3| < \frac{1}{2}p^2 + p^{\frac{5}{3}} + \frac{1}{2}p^{\frac{4}{3}} < p^2.$$

Which is saying that if $p > 15$, we can make $j = \lceil p^{\frac{1}{3}} \rceil$ queries in the same fashion as Lemma 2.1.3, and there still will be subgroups left to check. ∎

In fact, we wrote a code in Python in order to obtain some experimental data, and see whether, in practice, we can perform more than the number of queries as in Lemma 2.3.14. We generated the following graph showing the number of queries we can perform in the same fashion as Lemma 2.1.3 for different primes.

Note that the number of queries that we can perform in the same fashion as Lemma 2.1.3 is not only greater than $j = p^{\frac{1}{3}}$, but it is in fact close to $10^{\frac{1}{4}}p^{\frac{4}{10}}$.

Proposition 2.3.15. *Let $p > 15$ be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then the above algorithm to find a hidden subgroup of G uses at most $\lfloor p^{\frac{1}{3}} \rfloor + \frac{p-\sqrt{p}+2}{4}$ queries to the hiding function.*

Proof: The number of queries using Algorithm 2.3.13 is

$$X = j + \frac{(p+1) - \frac{j(j+1)}{2}}{2},$$

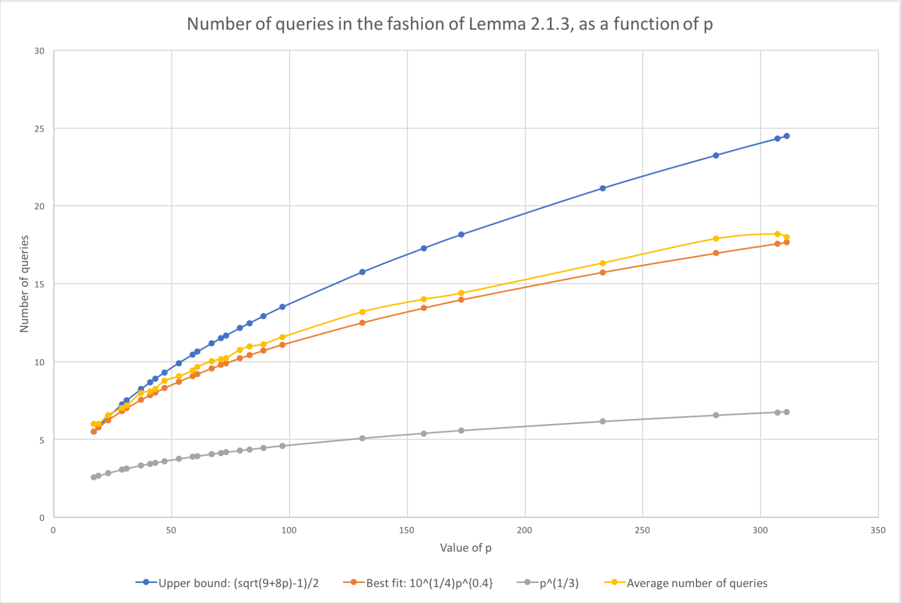


Figure 2.1: The graph is due to Anna Kis. Each point on the graph represents an average of the outputs produced for a certain prime. The code was executed 500 times for primes $p < 48$, 250 times for primes $48 < p < 100$, and approximately 5 times for primes $p > 130$.

where j queries are performed as outlined in Lemma 2.1.3 and once it is not possible to query elements g_j such that $g_j \notin g_k + \langle g_s - g_t \rangle$, for all $0 \le k, s, t < j$, we perform the remaining queries as outlined in Lemma 2.3.12.

If $j = \lfloor p^{\frac{1}{3}} \rfloor$ by Lemma 2.3.14, then $X = j + \frac{(p+1)-\frac{j(j+1)}{2}}{2}$ is bigger than $\lfloor p^{\frac{1}{3}} \rfloor + \frac{(p+1)-l}{2}$. Which in turn is bigger than $\lfloor p^{\frac{1}{3}} \rfloor + \frac{p-\sqrt{p}+2}{4}$, since $j = \lfloor p^{\frac{1}{3}} \rfloor < p^{\frac{1}{2}}$. So we need to perform more than $\lfloor p^{\frac{1}{3}} \rfloor + \frac{p-\sqrt{p}+2}{4}$ queries. ∎

2.3.4 The case of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$, for a prime p.

In this section we will focus on the case $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ and try to apply methods from the previous case to the current one. As always, we are interested in the subgroup structure of the group. The following theorem outlines the subgroup structure of $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$.

Lemma 2.3.16. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Then there are $2p + 4$ subgroups of G and all subgroups of G belong to one of the following classes.*

1. $\{(0,0)\}$ *there is one such subgroup. The order of* $\{(0,0)\}$ *is one.*

2. *$\langle(1,0)\rangle$ there is one such subgroup. It is cyclic of order p.*

3. *$\langle(a,p)\rangle$, where $a \in \mathbb{Z}/p\mathbb{Z}$, there are p such subgroups. Each such subgroup is cyclic of order p.*

4. *$\langle(a,1)\rangle$, where $a \in \mathbb{Z}/p\mathbb{Z}$, there are p such subgroups. Each such subgroup is cyclic of order p^2.*

5. *$\langle(0,p),(1,0)\rangle$, there is one such subgroup. The order of $\langle(0,p),(1,0)\rangle$ is p^2. This subgroup is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

6. *G, the whole group.*

Proof:

Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. We will classify all the subgroups of G.

Before we begin the proof, let us state some useful facts that we will use many times throughout this proof. Suppose $\gcd(s,p) = 1$. Then s is invertible modulo p^2, that is, there exists $t \in \mathbb{Z}$ such that $ts \equiv 1 \pmod{p^2}$, and so we also have $st \equiv 1 \pmod{p}$. Therefore for any $(a,b) \in G$ we have

$$\gcd(s,p) = 1 \implies \langle(a,b)\rangle = \langle(sa,sb)\rangle. \tag{2.3.6}$$

This is because $s(a,b) = (sa,sb)$ so $(sa,sb) \in \langle(a,b)\rangle$ and $t(sa,sb) = (tsa,tsb) = (a,b)$ since $ts \equiv 1$ in both $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$, so $(a,b) \in \langle(sa,sb)\rangle$.

We begin our proof with the cyclic subgroups

Let $(a,b) \in G$. If $b = a = 0$, then the subgroup $\langle(a,b)\rangle$ is the trivial subgroup $\langle(0,0)\rangle = \{(0,0)\}$.

If $b = 0, a \neq 0$, then order of $(a,0)$ is p. Thus, the subgroup generated by $(a,0)$ is $\langle(a,0)\rangle = \langle(1,0)\rangle$.

If $b \neq 0$, then the order of b is either p or p^2. If the order of b is p, then $b = pk$, for some positive integer k such that $gcd(p,k) = 1$. In this case the subgroup generated by (a,b) is $\langle(a',p)\rangle$, where $a' = la$, such that $kl \equiv 1(\text{mod } p)$ by (2.3.6). There are p subgroups of this form since all the subgroups of this form are given by $\langle(a',p)\rangle$, where $a' \in \mathbb{Z}/p\mathbb{Z}$, and $\langle(a',p)\rangle \neq \langle(a'',p)\rangle$ if $a' \not\equiv a''(\text{mod } p)$.

Otherwise, the order of b is p^2, and so b is such that $gcd(b,p) = 1$. Let s be such that $sb \equiv 1(\text{ mod } p^2)$, then $s(a,b) = (a',1)$ since $gcd(b,p) = 1$ by (2.3.6). So the subgroups of this form can be written as $\langle(a',1)\rangle$, where $a' \in \mathbb{Z}/p\mathbb{Z}$. These subgroups are cyclic of order p^2. There are a total of p subgroups of this form.

We will now calculate subgroups of G of the form $\langle(a,b),(c,d)\rangle$, where $(a,b),(c,d) \in G$. We may assume without loss of generality that $a = 0(\text{mod } p), c \neq 0(\text{mod } p)$. That is because if $a = c = 0(\text{mod } p)$, then $\langle(a,b),(c,d)\rangle = \langle(0,b),(0,d)\rangle = \langle(0,gcd(b,d)\rangle$, and we have already covered this case. Also, if $a \neq 0(\text{mod } p), c \neq 0(\text{mod } p)$, then there exist $k \in \mathbb{Z}$ such that $ka = c(\text{mod } p)$. Then the subgroup $\langle (a,b),(c,d)\rangle = \langle (0, kb-d)\rangle$ by Lemma 2.2.12. Note that $gcd(k,p) = 1$. We have already covered this case.

So now if $a = 0(\text{mod } p), c \neq 0(\text{mod } p)$, we can without loss of generality replace the generator (c,d) with $(1,d')$, where $d' \in \mathbb{Z}/p^2\mathbb{Z}$ by (2.3.6).

If $b = kp$, for some positive integer k such that $gcd(k,p) = 1$, then $\langle (0,b),(1,d')\rangle = \langle (0,p),(1,d')\rangle$ by (2.3.6). Now, if $d' = 0(\text{ mod } p)$, then $\langle (0,p),(1,d')\rangle = \langle (0,p),(1,0)\rangle$. The subgroup $\langle (0,p),(1,0)\rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ as the the product of two cyclic subgroups of order p.

Otherwise, if $d' \neq 0(\text{mod } p)$, then by (2.3.6), $\langle (1,d')\rangle = \langle (m,1)\rangle$, where $md \equiv 1(\text{ mod } p^2)$. But since $(0,p) \in \langle (m,1)\rangle$, the subgroup $\langle (0,p),(1,d)\rangle = \langle (1,d)\rangle$. We have already covered this case.

If $gcd(b,p) = 1$, then $\langle ((0,b),(1,d')\rangle = \langle (0,1),(1,0)\rangle$ by (2.3.6). This will be the whole group G

So there are $2p+4$ subgroups in total. ∎

Note that some of the subgroups share a common element, so we can not directly apply methods from the previous section.

Corollary 2.3.17. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. There are $p+3$ subgroups of G that contain the element $(0,p)$.*

Proof: Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. We will show that there are $p+3$ subgroups that contain the element $(0,p)$.

First, the subgroup $\langle (0,p)\rangle$ contains the element $(0,p)$.

All the subgroups of the form $\langle (a,1)\rangle$, where $a \in \mathbb{Z}/p\mathbb{Z}$ also contain $(0,p)$. By Lemma 2.3.16, there are p of these subgroups.

The subgroup $\langle (0,p),(1,0)\rangle$ and the entire group G also contain $(0,p)$.

By Lemma 2.3.16 other subgroups do not contain $(0,p)$. ∎

Interestingly, since there are $2p+4$ subgroups in total, and $p+3$ subgroups contain $(0,p)$, we can conclude than more half of the subgroups contain $(0,p)$.

Lemma 2.3.18. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Let $K = \langle (0,p)\rangle$. There exists an isomorphism between G/K and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proof: Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Let $K = \langle (0,p)\rangle$.

Let $\pi : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be the projection map, acting via $b \mapsto b(\text{ mod} p)$. Note that π is a well-defined homomorphism, since if a and b are congruent mod p^2 then they are certainly congruent mod p. The map π is also surjective since for every $b \in \mathbb{Z}/p\mathbb{Z}$ we may choose an integer B representing the class of b, and then the class of $B(\bmod p^2)$ is an element of $\mathbb{Z}/p^2\mathbb{Z}$ that maps to b. The kernel of this map is $\{pc|c \in \mathbb{Z}/p^2\mathbb{Z}\}$.

Now define $\phi\colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by $\phi(a,b) = (a, \pi(b))$. The kernel is $\{(a,b) \mid a = 0(\bmod p) \text{ and } \pi(b) = 0(\bmod p^2)\} = \{(0,pc) \mid c \in \mathbb{Z}/p^2\mathbb{Z}\} = K$. It is surjective since for each $(a,c) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, we can choose $c' \in \mathbb{Z}/p^2\mathbb{Z}$ such that $\pi(c') = c$. Then $\phi(a,c') = (a,c)$.

By the First Isomorphism Theorem 2.2.14, we conclude that there exists an isomorphism between G/K and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

∎

Lemma 2.3.19. *Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Let H be the hidden subgroup. Let $f : G \to X$ be a function, hiding H. Suppose that $K = \langle(0,p)\rangle \subseteq H \subseteq G$, then f gives a hiding function of H/K in G/K.*

Proof: Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Let H be the hidden subgroup. Let $f : G \to X$ be a function, hiding H. Suppose that $K = \langle(0,p)\rangle \subseteq H \subseteq G$.

Let $\pi\colon G \to G/K$ be the projection map and define a new function $\overline{f}\colon G/K \to X$ by $\overline{f}(gK) = f(g)$. Let us check this is well-defined. Since $K \subseteq H$, if $gK = g'K$ then $g^{-1}g' \in K \subseteq H$ so since f hides H, we know that $f(g) = f(g')$. So $\overline{f}$ is well-defined.

Now let us check that $\overline{f}$ hides H/K. Recall that $H/K = \{hK \in G/K \mid h \in H\}$. If $\overline{f}(gK) = \overline{f}(g'K)$ then $f(g) = f(g')$ so $g^{-1}g' \in H$ and thus $g^{-1}g'K = (gK)^{-1}(g'K) \in H/K$. Conversely, if gK and $g'K$ are two elements of G/K giving the same coset of H/K, then $(gK)^{-1}(g'K) \in H/K$ so $g^{-1}g' \in H$, and thus $f(g) = f(g')$, so $\overline{f}(gK) = \overline{f}(g'K)$.

∎

Let p be a prime. Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$. Let H be the hidden subgroup. Let $f : G \to X$ be a function, hiding H. The following steps compose an algorithm to solve the HSP over $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$.

The first step is to query the identity element $(0,0)$ and the element $(0,p)$. By Corollary 2.3.17, we know that the second query divides the set of all subgroups roughly in half.

If $f(0,0) = f(0,p)$ then the hidden subgroup H contains the element $(0,p)$. This implies that $K = \langle(0,p)\rangle \subseteq H$. By Lemma 2.3.19, the function f induces a function $\overline{f}\colon G/K \to X$ that hides H/K. By Lemma 2.3.18, there is an isomorphism $\phi\colon G/K \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Therefore the function $f' = \overline{f}\colon \phi^{-1}\colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to X$ is a hiding function for $E = \phi(H/K) \subseteq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Apply now the HSP algorithm for $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ from Section 1.3.3. It yields the hidden subgroup E. Apply ϕ^{-1} to E to find H/K. Finally apply Theorem 2.2.15 to recover H.

Concretely, if E is the trivial subgroup then $H = K$; if $E = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ then $E = G$. Otherwise, if $E = \langle (a, b) \rangle$ then choose any integer B whose reduction mod p is b; then $H = \langle (a, B) \rangle$.

If $f(0, 0) \neq f(0, p)$, then H does not contain the element $(0, p)$. There are $p + 2$ subgroups that do not contain $(0, p)$ by Corollary 2.3.17, namely $\langle (0, 0) \rangle$, $\langle (1, 0) \rangle$, and subgroups of the form $\langle (a, p) \rangle$, where $a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$.

Let $\mathcal{H} \leq G$ be the subgroup of the form $\mathcal{H} = \langle (0, p), (1, 0) \rangle$. Then $\psi : \mathcal{H} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ via $(a, bp) \mapsto (a, b)$, is an isomorphism. Since $\psi^{-1} : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathcal{H}$ via $(a, b) \mapsto (a, bp)$ is a well-defined map, and $(a, bp) + (c, dp) = (a + c, (b + d)p) \mapsto \psi(a + c, (b + d)p) = (a + c, b + d) = (a, c) + (b, d)$.

Now if H is one of the subgroups not containing $(0, p)$, then we see from Corollary 2.3.17 that $H \subset \mathcal{H}$. Therefore restricting f to $\mathcal{H}$ gives a hiding function $f|_{\mathcal{H}} \colon \mathcal{H} \to X$ that hides H. Composing with the isomorphism $\psi \colon \mathcal{H} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ gives a hiding function $f' = f|_{\mathcal{H}} \circ \psi^{-1} \colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to X$, which hides the subgroup $E = \psi(H)$.

Apply now the HSP algorithm for $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ from Section 1.3.3. It yields the hidden subgroup E. Apply ψ^{-1} to E to find H.

Concretely, if E is the trivial subgroup then so is H. Otherwise, if $E = \langle (a, b) \rangle$ then $H = \langle (a, bp) \rangle$.

Remark 2.3.20. We believe that similar algorithms can be applied to the case $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$, for any k to reduce the case to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and solve for the hidden subgroup in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

2.4 Classical query complexity of the Hidden Subgroup Problem over dihedral groups

We will now turn our attention to a more interesting class of groups, nonabelian groups. In this section we will only consider dihedral groups. The case of Dihedral HSP is of most interest and importance to us, since there are promising applications of the Dihedral HSP to post-quantum cryptography [11].

2.4.1 Dihedral groups

Definition 2.4.1. The dihedral group D_{2n} is the group of all rotations and reflections of an n-gon. As a group it is generated by two elements, r and s, subject to the relations $r^n = s^2 = rsrs = 1$, so we denote it by $D_{2n} = \langle r, s \mid r^n = s^2 = rsrs = 1 \rangle$. As a set we have $D_{2n} = \{r^k, r^k s \mid 0 \leq k < n\}$.

Let us note a few consequences of this definition. For one, let us show that for any $i \in \mathbb{Z}$ the order of $r^i s$ is 2. By the definition of D_{2n} we have $rsrs = 1$ which implies $rsr = s^{-1}$. Since $s^2 = 1$ this gives $rsr = s$. It follows by induction that $r^isr^i = s$ for any $i \geq 1$ and therefore that $r^isr^is = 1$. Since $r^n = 1$, $r^{-1} = r^{n-1}$ so this result holds for negative powers i as well. Thus $(r^is)^2 = 1$. The definition assures us that $r^is \neq 1$, so this element has order 2.

Another consequence is that for any integers l, k we have

$$r^lsr^k = r^{l-k}r^ksr^k = r^{l-k}s.$$

Theorem 2.4.2. *The dihedral group D_{2n} has two kinds of subgroups, and every subgroup of D_{2n} occurs once in this list:*

For each $d|n$, a subgroup of the form $\langle r^d\rangle$. This is a cyclic subgroup of order n/d.

For each $d|n$ and $0 \leq e < d$, a subgroup of the form $\langle r^d, r^es\rangle$. This is a dihedral group isomorphic to $D_{2(n/d)}$.

Proof: Assume $H \subseteq \langle r\rangle$, then H has form $\langle r^d\rangle$ where $d|n$ and the result of the theorem is true.

Now assume that $H \nsubseteq \langle r\rangle$, then there exists some $0 \leq i < n$ such that $r^is \in H$. Note that the order of r^is is 2.

If $H = \langle r^is\rangle$ we are done because we can rewrite H as $\langle r^n, r^is\rangle = \langle 1, r^is\rangle$ and since $0 \leq i < n$, we satisfy the conditions of the theorem.

Now suppose there exist $k, l \in \{0, 1, \cdots, n-1\}$ such that $H = \langle r^ls, r^ks\rangle$. Set $t = l - k \pmod n$. Then by the calculations above, we have $r^lsr^ks = r^t$. Therefore by Lemma 2.2.12 we have $H = \langle r^t, r^ks\rangle$. Furthermore, let $d = \gcd(t, n)$. Then $\langle r^t\rangle = \langle r^d\rangle$, and so $H = \langle r^d, r^ks\rangle$.

Therefore for if H is generated by two elements we only need to consider the case of $H = \langle r^d, r^ks\rangle$ where $d|n$ and $k \geq 0$. Divide k by d to get $k = jd + e$ where $j \geq 0$ and $0 \leq e < d$. Then

$$r^es = r^{-dj+k}s = (r^d)^{-j}(r^ks) \in H,$$

and by Lemma 2.2.12, $H = \langle r^d, r^es\rangle$, as required.

Now suppose that H is generated by more than two elements. Suppose $H = \langle r^{v_1}, r^{v_2}, \ldots, r^{v_k}, r^{w_1}s, \ldots, r^{w_m}s\rangle$ for $v_1, \ldots, w_m$ in $[0, n-1]$. Then consider all possible subgroups of the form $\langle r^{w_i}s, r^{w_j}s\rangle$ where $i, j \in \{1, \ldots, m\}$. By above, such subgroups are equal to $\langle r^es, r^u\rangle$ for some $u \in [0, n-1]$ and minimal $e \in [0, n-1]$. Therefore, $H = \langle r^{u_1}, \ldots, r^{v_1}, \ldots, r^{v_k}, r^es\rangle$ for the minimal choice of e in $[0, n-1]$. We can use lemma 2.2.12 again, to express H as $\langle r^{d'}, r^es\rangle$ where $d'|n$. And by above, we can rewrite is as $H = \langle r^d, r^es\rangle$ such that $0 \leq e < d$.

Now we will show that every subgroup of D_{2n} shows in the list only once. Subgroups of the form $\langle r^d\rangle$, for each $d|n$ are cyclic of order n/d, and therefore distinct. So each such subgroup only shows once in the list. As for the subgroups of the form $\langle r^d, r^es\rangle$, for each $d|n$ and $0 \leq e < d$, we will show that they are isomorphic to $D_{2(n/d)}$.

Let $R = r^d$, and $S = r^e s$. Then R has order n/d, S has order 2, and $RSRS = 1$. Therefore $H \cong D_{2(n/d)}$.

So all we need to show is that $\langle r^d, r^e s\rangle \neq \langle r^d, r^f s\rangle$ for any $d|n$ and $0 \leq e < f < d$. Assume that $\langle r^d, r^e s\rangle \neq \langle r^d, r^f s\rangle$ for some $d|n$ and $0 \leq e < f < d$. Then there exists a positive integer l such that $r^{dl+f}s = r^e s$, which implies that $dl + f \equiv e \pmod{n}$. This further implies that $f \equiv e \pmod{d}$. But then $f = e + dm$ for some integer m, and we have $0 \leq e < f < d$. This implies a contradiction, thus our assumption is wrong. So the dihedral groups are distinct for each $d|n$ and $0 \leq e < d$.

∎

Corollary 2.4.3. *Let $G = D_{2p}$ where p is a prime. Then G has $p + 3$ subgroups:*

- *The trivial subgroup $\langle 1\rangle$*
- *The cyclic subgroup $\langle r\rangle$*
- *The p cyclic subgroups generated by a reflection $\langle r^k s\rangle$, for $0 \leq k < p$*
- *The whole group D_{2p}.*

Let n be a positive integer. The function $\tau(n) = \sum_{d|n} 1$ is called the divisor function, and the map $\sigma(n) = \sum_{d|n} d$ is called the sum of divisors function.

Lemma 2.4.4. *Let n be a positive integer. The maps $\tau(n)$, and $\sigma(n)$ are multiplicative functions. Suppose $n = {p_1}^{k_1} \ldots {p_m}^{k_m}$ is a prime factorization of n. Then $\tau(n) = \prod_{i=1}^m (k_i + 1)$, and $\sigma(n) = \prod_{i=1}^m (\frac{{p_i}^{k_i+1}-1}{p_i - 1})$.*

Proof: Recall that a function $\rho\colon \mathbb{N} \to \mathbb{Z}$ is multiplicative if for all pairs of relatively prime integers m, n we have $\rho(mn) = \rho(m)\rho(n)$, and $\rho(1) = 1$.

Note that $\tau(1) = 1$ and $\sigma(1) = 1$, since 1 has only one divisor, namely itself.

Now let n and m be positive, relatively prime integers. Consider

$$\tau(nm) = \sum_{d|nm} 1 = \sum_{d_i|n,\ dj|m} 1 = \sum_{d_i|n} (\sum_{d_j|m} 1) = \sum_{d_i|n} \tau(m) = \tau(m) \sum_{d_i|n} 1 = \tau(m)\tau(n).$$

Next consider

$$\sigma(nm) = \sum_{d|nm} d = \sum_{d_i|n, d_j|m} d_i d_j = \sum_{d_i|n} d_i (\sum_{d_j|m} d_j) = \sum_{d_j|m} d_j \sum_{d_i|n} d_i = \sigma(m)\sigma(n).$$

Suppose $n = {p_1}^{k_1} \dots {p_m}^{k_m}$ is a prime factorization of n. Then

$$\tau(n) = \tau({p_1}^{k_1} \dots {p_m}^{k_m}) = \tau({p_1}^{k_1}) \dots \tau({p_m}^{k_m}). \tag{2.4.1}$$

Since the divisors of ${p_i}^{k_i}$ are $\{1, p, \dots, p_i\}$, for any $i \in \{1, p_i, \dots, {p_i}^{k_i}\}$, then $\tau({p_i}^{k_i}) = (k_i + 1)$. So the equation (2.4.1) continues as

$$\tau(n) = (k_1 + 1) \dots (k_m + 1) = \prod_{i=1}^{m} (k_i + 1).$$

Similarly, for $n = {p_1}^{k_1} \dots {p_m}^{k_m}$ notice that

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

as a partial sum of geometric series. Thus,

$$\begin{aligned} \sigma(n) &= \sigma({p_1}^{k_1} \dots {p_m}^{k_m}) = \sigma({p_1}^{k_1}) \dots \sigma({p_m}^{k_m}) \\ &= \frac{{p_1}^{k_1+1} - 1}{p_1 - 1} \dots \frac{{p_m}^{k_m+1} - 1}{p_m - 1} = \prod_{i=1}^{m} \frac{{p_i}^{k_i+1} - 1}{p_i - 1}. \end{aligned}$$

▮

Lemma 2.4.5. *The total number of subgroups of D_{2n} is $\tau(n) + \sigma(n)$.*

Proof: By 2.4.2 D_{2n} has two types of subgroup. We will count how many subgroups of each type does D_{2n} have. There is one cyclic subgroup for each divisor of n. Therefore there are $\tau(n)$ such subgroups.

There are d dihedral groups corresponding to each divisor d of n, so there are $\sigma(n)$ such subgroups.

▮

Now that we are acquainted with the subgroup structure of the group D_{2n}, we will state some more results about subgroups and cosets of D_{2n}.

Lemma 2.4.6. *Let $G = D_{2p}$, where p is prime. Suppose that H is a subgroup of G. If $r^k sH = r^l sH$, for some $0 \leq k \neq l \leq n$, then $H = \langle r \rangle$ or $H = G$.*

Proof: Let H be a subgroup of G such that $r^k sH = r^l sH$. This implies that $(r^k s)^{-1} r^l s \in H$. Since $(r^k s)^{-1}(r^l s) = sr^{l-k}s = r^{k-l}$, and $k - l \not\equiv 0 (\text{mod } p)$, r^{k-l} generates $\langle r \rangle$ so $\langle r \rangle \subseteq H$. By the Theorem 2.4.2 if $\langle r \rangle \subseteq H$, then H must be $\langle r \rangle$ or G. ▮

Lemma 2.4.7. *Let $G = D_{2p}$, where p is prime. Suppose that H is a subgroup of G. If $r^l H = r^k sH$, then $H = \{1, r^{k-l}s\} = \langle r^{k-l}s \rangle$ or $H = G$.*

Proof: Suppose $r^l H = r^k sH$. Then $r^{-l}r^k s \in H$ and therefore $r^{k-l}s \in H$. By the Corollary 2.4.2, the only subgroups that contain $r^{k-l}s$ are $H = \langle r^{k-l}s \rangle$ and $H = G$. ▮

Lemma 2.4.8. *Let $G = D_{2n}$. Let $g, h \in G$. If $g^{-1}h = r^k s$, for some $0 \leq k < n$ it must be that $g = r^i$ and $h = r^j s$ or vice versa such that $k = j - i$ for some $0 \leq i, j < n$.*

Proof: Suppose $g = r^i$ and $h = r^j$ for some $0 \leq i, j < n$. Then $g^{-1}h = r^{j-i} = r^l$.

Suppose $g = r^i s$ and $h = r^j s$, for some $0 \leq i, j < n$. Then $g^{-1}h = r^{i-j} = r^m$.

Suppose $g = r^i s$ and $h = r^j$ for some $0 \leq i, j < n$. Then $g^{-1}h = r^{i-j}s = r^m s$. Note that it this case, $g^{-1}h = h^{-1}g$. ▮

2.4.2 The case of D_{2n} for various n.

Before we study classical algorithms to solve the HSP over D_{2n}, let us consider the following example.

Let $G = D_4$. Let H be the hidden subgroup. Let X be a finite set. Let $f : G \to X$ be the function hiding H. By Lemma 2.4.5, G has 5 subgroups. Namely, $\langle 1 \rangle$, $\langle r \rangle$, $\langle s \rangle$, $\langle rs \rangle$, and the entire group G. The most straightforward way to the solve the HSP would be to query the identity element, and then query generators $1, s, rs$ in order to find H. In the worst case, this approach requires 4 queries.

Since we have queried each element of the group, we cannot be satisfied with this attack. Ideally, we would like the number of queries to be as close to the bound in the Theorem 2.1.2 as possible. If $G = D_4$, the maximal number of subgroups that intersect trivially is 3, namely $\langle r \rangle, \langle s \rangle, \langle rs \rangle$. So we would like the attack that takes approximately three queries.

Consider the following attack. Query three elements $1, r$, and rs. Recall that $f(g) = f(g')$ if and only if $g^{-1}g' \in H$. So if for any $g_1 \neq g_2 \in \{e, r, rs\}$ we have $f(g_1) = f(g_2)$, then we are done. On the other hand, if none of the three values match, then we are done as well. Since the only way this is the case, is when $H = \langle 1 \rangle$.

Note how knowing functional value of some elements has helped us eliminate more than one subgroup at a time. To be more precise we used the the following result. If $f(a) = f(b)$, then $H = \langle a^{-1}b \rangle$. If $f(a) \neq f(b)$, then $H \neq \langle a^{-1}b \rangle$. The following Lemma is our first attempt at an efficient algorithm, and it shows precisely how to use this result.

Lemma 2.4.9. *Let $G = D_{2p}$, where p is an odd prime, and let $H \leq G$ be the hidden subgroup. There exists an algorithm solving the Hidden Subgroup Problem with at most $\frac{p+5}{2}$ queries.*

Proof: Let $G = D_{2p}$, where p is an odd prime, and let $H \leq G$ be the hidden subgroup. Let f be an H-periodic function. Recall that for any $g \in G$, $f(1) = f(g)$ if and only if $g \in H$. Therefore, the first step is to query $f(1)$, so that we can determine whether $g \in H$ from the value of $f(g)$.

Next, query $f(r)$. If $f(r) = f(1)$, then $H = \langle r \rangle$ or $H = D_{2p}$. So in case that $f(r) = f(1)$, we only need one query to determine H. In this case, we performed 3 queries in total. Since for any odd prime p, we have $3 \leq \frac{p+5}{2}$, the statement of the theorem is true.

If $f(r) \neq f(1)$, then H is either a trivial subgroup of a subgroup of the form $\langle r^k s \rangle$, for some $0 \leq k < p$. There are p such subgroups. Note that by Lemma 2.4.6 and Lemma 2.4.7 querying one element of the form $r^k s$, for some $0 \leq k < p$, eliminates two subgroups. If one of these subgroups is H, we needed at most $\frac{p-1}{2}$ queries to find it among all subgroups of the form $\langle r^k s \rangle$. In total we require less than $2 + \frac{p-1}{2}$ queries. Since $2 + \frac{p-1}{2}$ is less than $\frac{p+5}{2}$, the theorem is true.

Now assume that we performed $\frac{p-1}{2}$ queries and narrowed possibilities for H to $H = \langle r^e s \rangle$ or $H = \langle 1 \rangle$, for some $0 \leq e < p$. Now we will have to perform one last query to determine H. Thus, in total we require $1 + 1 + \frac{p-1}{2} + 1 = \frac{p+5}{2}$ queries. ∎

Note that for any positive integer n, the multiplicative cyclic group of n elements, C_n, is isomorphic to the group of rotations of $G = D_{2n}$. We will use C_n to denote the groups of rotations of D_{2n} in the context of dihedral groups.

Let $G = D_{2p}$, for some positive prime p. Corollary 2.4.3 lists all the subgroups of G. It is apparent from this list, that there are $p + 1$ non-trivial subgroups of G that intersect trivially. Namely, the subgroup $\langle r \rangle$, and all p subgroups of the form $\langle r^k s \rangle$, for some $0 \leq k < p$. Thus, by Lemma 2.1.2, we would like to solve the HSP using approximately $\sqrt{2(p+1)}$ queries. The following theorem describes an attack that takes at most $2\sqrt{p}$ queries to solve the HSP.

Theorem 2.4.10. *Let $G = D_{2p}$, where p is a prime, and let $H \leq G$ be a hidden subgroup. There exists an algorithm that finds H with at most $2\sqrt{p}$ queries.*

Proof: $G = D_{2p}$ for some positive prime p. Suppose $H \leq G$ is the hidden subgroup. Let X be a finite set, and let $f : G \to X$ be the function hiding H.

Let w denote $\lceil \sqrt{p} \rceil$. Let S be the set

$$S = \{e, r, r^2, r^3, \ldots, r^{w-1}; r^{w-1}s, r^{2w-1}s, r^{3w-1}s, \ldots, r^{kw-1}s; r^{p-1}s\}, \tag{2.4.2}$$

where k is the largest positive integer such that $kw < p$. Our algorithm is as follows. For each $g \in S$, evaluate $f(g)$ and store the pair $(g, f(g))$.

Note an interesting property of the elements that we queried. By taking any two elements $g, h \in S$ and producing an element $g^{-1}h \in G$, we can generate any possible reflection in D_{2p}. Let $g_i = r^i$ for $i \in \{0, \dots, w-1\}$ and $h_j = r^j s$ for $j \in \{w-1, 2w-1, 3w-1, \dots, kw-1; p-1\}$, then

$$g_i{}^{-1}h_j = r^{-i}r^j s = r^{j-i}s \text{ where } j-i \in \{0, 1, 2, \dots, p-1\}. \tag{2.4.3}$$

Recall that $gH = g'H$ if and only if $g^{-1}g' \in H$. So if $f(g) = f(g')$, then $g^{-1}g' \in H$. Now, in the case of dihedral groups, if one or more of the above queries are the same then either, $r^l \in H$ or $r^t s \in H$ for $t \in \{0, 1, \dots, p-1\}$ and $l \in \{1, 2, \dots, p-1\}$. If $r^i \in H$ for $l \in \{1, 2, \dots, p-1\}$, then by Lemma 2.4.2, we have $H \in \{\langle r\rangle, D_{2p}\}$. And since we have enough queries to distinguish between $H = \langle r\rangle$ and $H = D_{2p}$ we do not require any additional work.

If $r^t s \in H$ for $t \in \{0, 1, \dots, p-1\}$. Then by Lemma 2.4.2 $H \in \{\langle r^j s\rangle, D_{2p}\}$. In this case we also have enough queries to determine whether $H = \langle r^j s\rangle$ or $H = D_{2p}$ we will not perform any additional queries.

If none of the queries are the same, then $g_i{}^{-1}h_j \notin H$ for any $g_i, h_j \in S$. By (2.4.3), that would mean that none of the elements of the form $r^t s$, for any $t \in \{0, \dots, p-1\}$ are in H. Moreover, since $1, r \in S$, then $r \notin H$. By Lemma 2.4.2 that would mean that H is the trivial subgroup.

In total we made $2w$ queries. Note that such choice is optimal. Suppose that instead of $2w$ queries in total, we made $m \in \mathbb{Z}^+$ queries of rotations from e to r^{m-1}, and $\frac{p}{m}$ queries of reflections in the following fashion:

$$f(r^{m-1}s), f(r^{2m-1}), \dots, f(r^{dm-1}); f(r^{p-1}s), \tag{2.4.4}$$

for positive integer d such that $dm < p$. Then it would yield $m + \frac{p}{m}$ queries in total. Notice that the function $m + \frac{p}{m}$ reaches its minimum when $m = \sqrt{p}$. Thus, we need $m + \frac{p}{n} = \sqrt{p} + \frac{p}{\sqrt{p}} = 2\sqrt{p}$ queries in total. To make sure, we make an integer number of queries, we set the total number of queries to be $2\lceil\sqrt{p}\rceil$. ∎

We would like to generalize the following algorithm to the case $G = D_{2p^k}$, for some positive integer k. The following Lemma describes an optimal attack for the case $G = D_{2p^k}$, in the sense that the number of queries is approximately equal to the bound in the Theorem 2.1.2. By the Theorem 2.4.2, the only non-trivial subgroups of D_{2p^k} are the subgroup $\langle r\rangle$, and all p^k subgroups of the form $\langle r^l s\rangle$, for some $0 \leq l < p^k$. So the number of non-trivial subgroups of D_{2p^k} that intersect trivially is $p^k + 1$.

Proposition 2.4.11. *Let $G = D_{2p^k}$, for some positive prime p, and positive integer k. There exists an algorithm that solves the Hidden Subgroup Problem with at most $\lceil\log_2(k+1)\rceil + 2\sqrt{p^k}$ queries.*

Proof: Let $G = D_{2p^k}$, for some positive primes p, and positive integer k. Let $H \leq G$ be a hidden subgroup. Let X be a finite set. Let $f : G \to X$ be a function that is hiding the hidden subgroup H.

Our strategy is to discover, whether or not H contains a rotation. Once we determine that, we have some knowledge about the structure of H, and will be able to determine the best strategy to find H.

We start the algorithm by running a binary search on C_{p^k}. By Lemma 2.4.12, that will allow us to find $H \cap C_{p^k}$. The result $H \cap C_{p^k} = \{r^i\}$, for some $i \in \{1, p, p^2, \ldots, p^{k-1}, p^k\}$.

Let m be a positive integer. Let S be the set

$$S = \{e, r, r^2, \cdots, r^{m-1}; r^{m-1}s, r^{2m-1}, \cdots, r^{\frac{p^k}{m}m-1}s\}. \tag{2.4.5}$$

The second step of the algorithm is to evaluate $f(g)$ for each $g \in S$, and store the pair $(g, f(g))$. Recall that if $f(g_i) = f(g_j)$, then $g_iH = g_jH$ if and only if ${g_i}^{-1}g_j \in H$.

Suppose $H \cap C_{p^k} = \{r^{p^k}\} = \{e\}$. By Lemma 2.4.2

$$H = \langle r^j s\rangle \text{ for some } j \in \{0, 1, 2, \ldots, p^k - 1\} \text{ or } H = \{e\}.$$

Suppose that one or more queries of the elements in S are the same. Then it must be that $H = \langle r^j s\rangle$ for some $j \in \{0, 1, 2, \ldots, p^k - 1\}$, and we can determine H.

Suppose $H \cap C_{p^k} = \{r^{p^k}\} = \{e\}$, and none of the queries of the elements in S are the same, then H must be the trivial subgroup.

Suppose that $H \cap C_{p^k} = \{r^i\}$ for some $i \in \{1, p, p^2, \ldots, p^{k-1}\}$. Then by Lemma 2.4.2

$$H = \langle r^i\rangle \text{ or } H = \langle r^i, r^e s\rangle \text{ for } i \in \{1, p, p^2, \ldots, p^{k-1}\} \text{ and } 0 \leq e < i.$$

Note that every element of the form $r^j s$ for $j \in \{0, 1, 2, \ldots, p^k - 1\}$ can be expressed as a product ${g_i}^{-1}g_j$ where $g_i, g_j \in S$. Suppose that none of the queries of the elements in S are equal. Then $H = \langle r^i\rangle$, for some $i \in \{1, p, p^2, \ldots, p^{k-1}\}$, and we can determine H using information from our queries.

Suppose that $H \cap C_{p^k} = \{r^i\}$ for some $i \in \{1, p, p^2, \ldots, p^{k-1}\}$. If one or more queries are equal, then one or more elements of the form $r^j s$ for $j \in \{1, 2, \ldots, p^k - 1\}$ are in H then we can conclude that $H = \langle r^i, r^e s\rangle$, and find H using data from our queries.

By Lemma 2.3.8 in total, we needed to make $\lceil \log_2 (k + 1)\rceil + m + \frac{p^k}{m}$ queries in total. We would like to optimize this number of queries. Note that the function $m + \frac{p^k}{m}$ reaches its minimum when $m = \sqrt{p^k}$. Thus, with this result in total we need to perform $\lceil \log_2 (k + 1)\rceil + 2\sqrt{p^k}$ queries. ∎

Now that we have developed a successful strategy to solve the HSP for D_{2p^k}, we will tackle the case D_{2n}, for some positive integer n. Before we describe the algorithm to solve the HSP for D_{2n}, we will state a useful result that we will use in the algorithm.

Lemma 2.4.12. *Let $G = D_{2n}$, where n is some positive integer. Let $H \leq G$ be the hidden subgroup and let $f : G \to X$, where X is a finite set, be the function that hides H. Then $f|_{C_n}$ hides $H \cap C_n$.*

Proof: Let $G = D_{2n}$, where n is some positive integer. Let $H \leq G$ be the hidden subgroup and let $f : G \to X$, where X is a finite set, be the function that hides H. Suppose $a, b \in C_n$ and suppose that $f(a) = f(b)$. Then $aH = bH$ since f is H-periodic. It follows that $a^{-1}b \in H$, but since both $a, b \in C_n$ so is $a^{-1}b$. Thus, $a^{-1}b \in H \cap C_n$.

Suppose that $a, b \in C_n$ and $a(H \cap C_n) = b(H \cap C_n)$. Then $a^{-1}b \in H \cap C_n$. It follows that $a^{-1}b \in H$. But since f is H-periodic $a^{-1}b \in H$ means that $f(a) = f(b)$. Thus, $f|_{C_n}$ is $H \cap C_n$-periodic. ∎

Theorem 2.4.13. *Let $G = D_{2n}$, where n is some positive integer. Let $n = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of n. There exists an algorithm that solves the Hidden Subgroup Problem using at most $\lceil \log_2 (e_1 + 1) \rceil + \cdots + \lceil \log_2 (e_k + 1) \rceil + 2\sqrt{n}$ queries.*

Proof: Let n be a positive integer. Let $n = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of n. Let $G = D_{2n}$. Suppose $H \leq G$ is the hidden subgroup. Let X be a finite set. Let $f : G \to X$ be a function hiding H.

The first step of our algorithm is to run a binary search on C_n. By Lemma 2.4.12 we will find $H \cap C_n$. By Lemma 2.4.2, the group $H \cap C_n$ is $\{r^i\}$ for some $i \in \{1, d_1, d_2, \ldots, d_k\}$, where d_is are divisors of n.

Let m be a positive integer. Let S be the set

$$S = \{e, r, r^2, \cdots, r^{m-1}; r^{m-1}s, r^{2m-1}s, \cdots, r^{\frac{n}{m}m-1}s\} \tag{2.4.6}$$

The second step of the algorithm is to evaluate $f(g)$ for each $g \in S$, and store the pair $(g, f(g))$. Recall that if $f(g_i) = f(g_j)$, then $g_iH = g_jH$ if and only if ${g_i}^{-1}g_j \in H$.

If $H \cap C_n = \{r^n\} = \{e\}$, then by Lemma 2.4.2, $H = \langle r^j s\rangle$ for some $j \in \{0, 1, 2, \ldots, n-1\}$ or $H = \{e\}$. Suppose that one or more queries in S are the same. Then H is r^js for $j \in \{0, \ldots, n-1\}$, and we can conclude what H is.

Suppose that $H \cap C_n = \{e\}$ and suppose that none of the queries are the same. That would mean that ${g_i}^{-1}g_j \notin H$ for any $g_i, g_j \in S$. By Lemma 2.4.2 that would mean that H is a trivial subgroup.

Suppose $H \cap C_n = \{r^i\}$ for some $i \in \{1, d_1, d_2, \ldots, d_k\}$, where $d_i \neq n$ are divisors of n. Then by Lemma 2.4.2, $H = \langle r^i\rangle$ or $H = \langle r^i, r^e s\rangle$ for $i \in \{1, d_1, d_2, \ldots, d_k\}$ and $0 \leq e < i$. Suppose two or more queries in S are equal. Note that every element of the form r^js for $j \in \{0, 1, \ldots, n-1\}$ can be expressed as a product ${g_i}^{-1}g_j$ where $g_i, g_j \in S$. Thus, after performing the second step we know precisely what elements of the form r^js for $j \in \{1, 2, \ldots, n-1\}$ are the members of H. So we can conclude what H is.

Suppose $H \cap C_n = \{r^i\}$ for some $i \in \{1, d_1, d_2, \ldots, d_k\}$, where $d_i \neq n$ are divisors of n. Suppose none of these elements are in H we can conclude that $H = \langle r^i \rangle$ since $H \cap C_n = \{r^i\}$.

By Lemma 2.3.8, we needed to make $\lceil \log_2(e_1 + 1) \rceil + \cdots + \lceil \log_2(e_k + 1) \rceil + m + \frac{n}{m}$ queries in total. We would like to optimize this number of queries. Note that the function $m + \frac{n}{m}$ reaches its minimum when $m = \sqrt{n}$. Thus, with this result in total we need to perform $\lceil \log_2(e_1 + 1) \rceil + \cdots + \lceil \log_2(e_k + 1) \rceil + 2\sqrt{n}$ queries. ∎

We believe the result for D_{2n} is optimal assuming our algorithm for cyclic subgroups is optimal. Note that subgroups of D_{2n} of the form $\langle r^k s \rangle$, for some $0 \leq k < n$ are non-trivial and they intersect trivially. So the number of non-trivial subgroups of D_{2n} that intersect trivially is at least n. So the bound from Theorem 2.1.2 in case $G = D_{2n}$ is more than $\sqrt{2n}$. Our bound is $\lceil \log_2(e_1 + 1) \rceil + \cdots + \lceil \log_2(e_k + 1) \rceil + 2\sqrt{n}$.

Chapter 3

Quantum algorithms for the Hidden Subgroup Problem

We are now moving forward to the second part of this thesis - quantum algorithms to solve the HSP. We are going to briefly talk about quantum algorithms for the HSP over finite abelian groups but the main focus for us will be HSP over dihedral groups. The case of the dihedral group is particularly of interest to us since there are useful applications of the Dihedral HSP to cryptography. We will consider some of the existing algorithms to solve the HSP and introduce our own.

3.1 Background

Let us begin with a recap of some useful results from representation theory and quantum computing.

3.1.1 Representation theory of finite groups

The following subsection is based on a wonderful textbook by Jean-Pierre Serre [23]. Many proofs given here are inspired by the proofs in that book.

Definition 3.1.1. A (complex) representation ρ of a group G is a homomorphism $\rho : G \to GL(V)$, where V is a vector space over $\mathbb{C}$. The dimension d_ρ of the representation is defined to be to the dimension d of V. We will refer to d as the dimension or the degree of ρ.

Example. Let $G = C_7$ be a cyclic group of order 7, generated by g. Let us find all the 1-dimensional representations χ of G.

Since $g^7 = 1$ and χ is a homomorphism, we have $\chi(g)^7 = \chi(g^7) = \chi(1) = 1$. This implies that the values of χ are precisely the 7-th roots of unity, namely $1, e^{\frac{2\pi i}{7}}, e^{\frac{4\pi i}{7}}, e^{\frac{6\pi i}{7}}, e^{\frac{8\pi i}{7}}, e^{\frac{10\pi i}{7}}, e^{\frac{12\pi i}{7}}$.

Moreover, note that in order to specify χ, it suffices to determine only $\chi(g)$, since $\chi(g^k) = \chi(g)^k$, for any integer k. All seven representations and their values are in the table below.

	1	g	g^2	g^3	g^4	g^5	g^6
χ_0	1	1	1	1	1	1	1
χ_1	1	$e^{\frac{2\pi i}{7}}$	$e^{\frac{4\pi i}{7}}$	$e^{\frac{6\pi i}{7}}$	$e^{\frac{8\pi i}{7}}$	$e^{\frac{10\pi i}{7}}$	$e^{\frac{12\pi i}{7}}$
χ_2	1	$e^{\frac{4\pi i}{7}}$	$e^{\frac{8\pi i}{7}}$	$e^{\frac{12\pi i}{7}}$	$e^{\frac{2\pi i}{7}}$	$e^{\frac{6\pi i}{7}}$	$e^{\frac{10\pi i}{7}}$
χ_3	1	$e^{\frac{6\pi i}{7}}$	$e^{\frac{12\pi i}{7}}$	$e^{\frac{4\pi i}{7}}$	$e^{\frac{10\pi i}{7}}$	$e^{\frac{2\pi i}{7}}$	$e^{\frac{8\pi i}{7}}$
χ_4	1	$e^{\frac{8\pi i}{7}}$	$e^{\frac{2\pi i}{7}}$	$e^{\frac{10\pi i}{7}}$	$e^{\frac{4\pi i}{7}}$	$e^{\frac{12\pi i}{7}}$	$e^{\frac{6\pi i}{7}}$
χ_5	1	$e^{\frac{10\pi i}{7}}$	$e^{\frac{6\pi i}{7}}$	$e^{\frac{2\pi i}{7}}$	$e^{\frac{12\pi i}{7}}$	$e^{\frac{8\pi i}{7}}$	$e^{\frac{4\pi i}{7}}$
χ_6	1	$e^{\frac{12\pi i}{7}}$	$e^{\frac{10\pi i}{7}}$	$e^{\frac{8\pi i}{7}}$	$e^{\frac{6\pi i}{7}}$	$e^{\frac{4\pi i}{7}}$	$e^{\frac{2\pi i}{7}}$

Definition 3.1.2. Let $\rho_1 : G \to GL(V)$ and $\rho_2 : G \to GL(W)$ be representations of G. We say that the two representations are isomorphic, when there exists an isomorphism $f : V \to W$ such that for every group element $g \in G$ and every $v \in V$, $\rho_2(g)f(w) = f(\rho_1(g)(w))$.

Now, if G is finite and V is of finite dimension d, then fixing a basis of V gives rise to a $d \times d$ invertible matrix $M_\rho(g)$ associated to each $g \in G$. To be more precise, the matrix $M_\rho(g)$ depends on the choice of basis. So instead of $M_\rho(g)$ we will write $\rho_B(g)$ if B is the basis. Note that the trace of this matrix is independent of the choice of basis. This allows us to make the following definition.

Definition 3.1.3. The character associated to a representation ρ of a group G is the complex-valued function defined by $\chi_\rho(g) = tr(\rho(g))$.

Since $tr(AB) \neq tr(A)tr(B)$ in general, a character is not *usually* a homomorphism.

Definition 3.1.4. A representation $\rho : G \to GL(V)$ is said to be irreducible, if there are no nonzero proper subspaces $W \subset V$ such that for all $g \in G$, $\rho(g)W \subseteq W$. We call the character of such a representation, an irreducible character.

Suppose that $\rho \colon G \to GL(V)$ is not an irreducible representation. Then there exists a nonzero proper subspace $V' \subset V$ such that ρ restricts to a representation $\rho' \colon G \to GL(V')$. Moreover, by [23, Section 1.4], there exists a complementary subspace V'' of V' in V such that $\rho(g)v \in V''$ for all $v \in V''$ and all $g \in G$. Write ρ'' for the restriction of ρ to V''. Then we have $\rho = \rho' \oplus \rho''$.

Repeating the decomposition process, we can decompose ρ as $\rho = \rho_1 \oplus \cdots \oplus \rho_k$, for some positive integer k. Each representation ρ_i is irreducible, and the decomposition is unique up to an isomorphism.

Example. Let G be a (finite) group. Let V be a vector space with basis $\{e_g \mid g \in G\}$. For each $g' \in G$, let $\rho(g')$ be the linear map of V into V which sends e_g to $e_{g'g}$. Let's show this is a representation of G, called the regular representation.

We have that $\rho(g') \in GL(V)$ for each $g' \in G$. For $g, g', g'' \in G$, we have

$$\rho(g'g'')(e_g) = e_{(g'g'')g} = e_{g'(g''g)} = \rho(g')(e_{g''g}) = \rho(g')(\rho(g'')e_g) = (\rho(g')\rho(g''))(e_g)$$

so ρ is a homomorphism, and so a representation.

Let us compute its character χ. If $g' = e$, the identity element, then $\rho(e) = I$, the identity matrix. Thus

$$\chi(e) = tr(\rho(e)) = tr(I) = \dim(V) = |G|.$$

On the other hand, if $g' \neq e$ then $\rho(g')e_g = e_{g'g} \neq e_g$ so the matrix representing $\rho(g')$ is a permutation matrix and has zeroes on the diagonal. Thus $\chi(g') = tr(\rho(g')) = 0$ for every $g' \neq e$.

The regular representation is not irreducible. For example, let

$$w = \sum_{g \in G} e_g$$

and let $W = \text{span}\{w\} \subset V$. Then for any $g' \in G$, we have

$$\rho(g')w = \sum_{g \in G} \rho(g')e_g = \sum_{g \in G} e_{g'g} = \sum_{h \in G} e_h = w$$

so W is an invariant subspace and the restriction of ρ to W is called the trivial representation. In fact, the decomposition of ρ into irreducible subrepresentations is well-known, namely $\rho = \oplus d_\sigma \sigma$, where the sum is over all irreducible representations σ of G [23, Section 1.4].

We will now shift our attention to an extremely useful result, Schur's lemma.

Theorem 3.1.5. *Let $(\rho_1, V), (\rho_2, W)$ be two irreducible representations of G. Let $f : V \to W$ be a linear map such that $\rho_2(g)f = f\rho_1(g)$, for all $g \in G$. Then*

1. *If ρ_1 and ρ_2 are not isomorphic, then $f = 0$.*

2. *If $V = W$ and $\rho_1 = \rho_2$, then f has form $f = \lambda I$, where λ is a scalar.*

So in short, the lemma states that any homomorphism between irreducible representations is either an isomorphism or zero. The proof of this well-known result may be found in [23, Section 2.2]

Lemma 3.1.6. *All irreducible representations of abelian groups are 1-dimensional.*

Proof: Let G be an abelian group. Let $\rho : G \to GL(V)$ be an irreducible representation of G.

Since G is abelian note that

$$\rho(g)\rho(g')v = \rho(gg')v = \rho(g'g)v = \rho(g')\rho(g)v,$$

for any $g, g' \in G$, and $v \in V$. Thus, by Schur's Lemma 3.1.5, we know that for any $g \in G$, $\rho(g)v = \lambda_g v$, for some complex number λ_g. So $\rho(g) = \lambda_g I$, for any $g \in G$. So every subspace of V is invariant.

But we are working with irreducible representations, that implies that $dim(V) = 1$ by Definition 3.1.4. ▮

A one-dimensional representation is a homomorphism $\chi\colon G \to GL(\mathbb{C})$. Since $GL(\mathbb{C}) = \mathbb{C}^*$ and since the trace of a 1×1 matrix is just the entry of the matrix, these representations are the same as their characters. This leads to the following definition of characters of finite *abelian* groups. Remember that in Definition 2.1.2, which concerns general finite groups, χ is not necessarily a homomorphism.

Definition 3.1.7. A character, χ, of an *abelian* group G is a homomorphism $\chi : G \to \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers. Therefore, for $a, b \in G$ and $n \in \mathbb{Z}$ the following is true

$$\chi(a + b) = \chi(a)\chi(b) \tag{3.1.1}$$

$$\chi(na) = (\chi(a))^n \tag{3.1.2}$$

Example. Let $G = C_7$ be a cyclic group of order 7, generated by g. The irreducible representations of C_7 are of degree 1. These representations ρ map g to complex number $\rho(g) = w$, and $\rho(g^k) = \rho(g)^k = w^k$. But note that $g^7 = 1$, thus $\rho(g)^7 = w^7 = 1$. From here we can conclude that $w = e^{\frac{2\pi i k}{7}}$, where $k \in \{0, \dots, 6\}$. Now we can actually see that irreducible representations of C_7 are given by the characters of C_7.

This example goes in line with what we have just discussed. If we think of C_7 as a general group, we define characters of C_7 as $\chi_\rho(g) = tr(\rho(g))$. Since all representations of C_7 are one-dimensional $tr(\rho(g)) = \rho(g)$.

Another important example is the trivial representation, $\rho : G \to GL(\mathbb{C})$ given by $\rho(g) = 1$ for all $g \in G$. The character of a trivial representation is the trivial character $\chi_0 = 1$.

Theorem 3.1.8. *Let G be a finite abelian group, and χ a character of G. Let χ_0 denote the trivial character. Then*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0 \end{cases}$$

Proof: Suppose that $\chi = \chi_0$, then $\sum_{g\in G} \chi(g) = \sum_{g\in G} 1 = |G|$.

Suppose that $\chi \neq \chi_0$ then there exists at least one $y \in G$ such that $\chi(y) \neq 1$. Note that $\sum_{g\in G} \chi(g)$ can be rewritten as $\sum_{z\in G} \chi(yz)$. Now,

$$\sum_{z\in G} \chi(yz) = \chi(y) \sum_{z\in G} \chi(z).$$

Since

$$\sum_{g\in G} \chi(g) - \sum_{z\in G} \chi(yz) = (1 - \chi(y)) \sum_{z\in G} \chi(z) = 0$$

and

$$\chi(y) \neq 1,$$

we can conclude that $\sum_{z\in G} \chi(z) = 0$. ∎

Definition 3.1.9. A class function f on G is a function that is constant on the conjugacy classes of G i.e. f is a class function on G if $f(ghg^{-1}) = f(h)$, for any $g, h \in G$.

Suppose that $\chi \colon G \to \mathbb{C}$ is the character of a representation $\rho \colon G \to GL(V)$. Then for any $g, h \in G$ we have

$$\chi(h^{-1}gh) = tr(\rho(h^{-1}gh)) = tr(\rho(h)^{-1}\rho(g)\rho(h)) = tr(\rho(g)) = \chi(g).$$

Therefore the characters of representations of G are class functions of G.

Definition 3.1.10. Let G be a finite group. We define an inner product on $\mathbb{C}^G$ by

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g\in G} f(g)\overline{f'(g)}$$

for each $f, f' \in \mathbb{C}^G$.

In particular, this definition implies that for any two characters of G,

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g\in G} \chi_1(g){\chi_2}^*(g), \qquad (3.1.3)$$

where ${\chi_2}^*(g) = \overline{\chi_2(g)}$.

The inner product defined in Definition 3.1.10 restricts to an inner product on the subspace of all class functions.

Let us give a name to the set of all irreducible characters of G, we call such set $\hat{G}$.

Lemma 3.1.11. *The irreducible characters of G, $\hat{G}$, form an orthonormal set in the space of class functions.*

The proof of this result can be found in [23, Section 2.3].

Theorem 3.1.12. *Let G be a group. The set $\hat{G} = \{\chi_0, \ldots, \chi_{N-1}\}$ is the set of all irreducible characters of G. Then $\hat{G}$ forms an orthonormal basis for the space of class functions on G, $Cl(G) = \{f : G \to \mathbb{C} | f(h^{-1}gh) = f(g), \ \forall g, h \in G\}$.*

Proof: Let G be a group. We will show that $\hat{G}$ forms an orthonormal basis for $Cl(G)$. First, notice that by Lemma 3.1.11, the elements of $\hat{G} = \{\chi_0, \ldots, \chi_{N-1}\}$ are orthonormal. Let ρ be an irreducible representation of G.

Now we will show that $\hat{G} = \{\chi_0, \ldots, \chi_{N-1}\}$ spans $Cl(G)$.

We will show that if $f \in Cl(G)$ is orthogonal to every $\chi_i \in \hat{G}$, for $i \in \{0, \ldots, N-1\}$, then f is a zero function. Define a linear map by $\rho_f = \sum_{g \in G} f(g)\rho(g)$ from V onto itself. Our first step is to show that it implies that ρ_f is zero.

Let any $g' \in G$. Then

$$\begin{aligned}
\rho_f \rho(g') &= \sum_{g \in G} f(g)\rho(g)\rho(g') \\
&= \sum_{g \in G} f(g)\rho(gg') \qquad \text{since } \rho \text{ is a homomorphism} \\
&= \sum_{g \in G} f(g)\rho(g'(g')^{-1}gg') \\
&= \sum_{g \in G} f(g)\rho(g')\rho((g')^{-1}gg') \\
&= \rho(g') \sum_{k \in G} f(g'k(g')^{-1})\rho(k) \qquad \text{where } k = (g')^{-1}gg' \\
&= \rho(g') \sum_{k \in G} f(k)\rho(k) \qquad \text{since } f \text{ is a class function} \\
&= \rho(g')\rho_f.
\end{aligned}$$

Therefore ρ_f satisfies the hypothesis of Schur's Lemma, so since ρ is irreducible, $\rho_f = \lambda I$ for some scalar λ.

Since ρ_f is a scalar matrix, its trace is λd where d is the degree of ρ. But since $tr(\rho(g)) = \chi(g)$ where χ is the character of ρ, we can compute

$$tr(\rho_f) = tr\left(\sum_{g \in G} f(g)\rho(g)\right) = \sum_{g \in G} f(g)\chi(g) = |G|\langle f, \overline{\chi}\rangle.$$

Finally, we note that if ρ is an irreducible representation, so is $\overline{\rho}$, so if χ is an irreducible character, then so is $\overline{\chi}$. Thus by hypothesis, this inner product is 0, so $\lambda = 0$.

Therefore, for every irreducible representation, we have shown that ρ_f is the zero transformation.

Now let ρ be the regular representation. Although ρ is not irreducible, it is the sum of irreducible representations, and by linearity we have that $\rho_f = 0$ as well. With respect to the basis $\{e_g \mid g \in G\}$ of the vectors space of ρ, we have that the image of e_{id} under ρ_f is $0 = \rho_f e_{id} = \sum_{g\in G} f(g)\rho(g)e_{id} = \sum_{g\in G} f(g)e_g$. Thus by linear independence of $\{e_g \mid g \in G\}$, we have $f(g) = 0$ for all $g \in G$. Hence f is the zero map. Since the orthogonal complement of the span of $\hat{G}$ is the zero space, we conclude that the span of $\hat{G}$ is all of $Cl(G)$, as required.

∎

Corollary 3.1.13. *Let G be a finite group. The number of conjugacy classes of G is equal to the number of the characters of the irreducible representations of G.*

Proof: By Theorem 3.1.12 we know that the number of irreducible characters of G is equal to the dimension of $Cl(G)$ because they form a basis for the space of class functions. Another basis for the space of class functions is given by letting $T = \{c_1, \cdots, c_N\}$ be the set of conjugacy classes of G and defining $f_i(g) = 1$ if $g \in c_i$ and $f_i(g) = 0$ if $g \notin c_i$. Therefore $|T| = |\hat{G}|$, that is, the number of irreducible characters is equal to the number of conjugacy classes of G. ∎

Corollary 3.1.14. *Let G be an abelian group. Let $\hat{G} = \{\chi_0, \ldots, \chi_{N-1}\}$ be the set of all characters of G. Then $\hat{G}$ forms a basis for all complex valued functions on G, $\mathbb{C}^G = \{f : G \to \mathbb{C} | f \text{ is a function }\}$.*

Proof: Suppose G is an abelian group. Then for every $g, h \in G$, we have $h^{-1}gh = g$ and so every function in $\mathbb{C}^G$ is a class function. Since $Cl(G) = \mathbb{C}^G$, Theorem 3.1.12 tells us that $\hat{G}$ is a basis for $\mathbb{C}^G$. ∎

Therefore we have shown that if G is abelian, then $|G| = |\hat{G}|$. In Example 3.1.1 we found 7 irreducible characters of C_7, and in fact they were indexed by elements of G is a nice way. This is a general fact.

Lemma 3.1.15. *Let $N > 1$. Then the map $\mathbb{Z}/N\mathbb{Z} \to \widehat{\mathbb{Z}/N\mathbb{Z}}$ given by $x \mapsto \chi_x$ where $\chi_x(y) = e^{2\pi i xy/N}$ for all $y \in \mathbb{Z}/N\mathbb{Z}$ is an isomorphism.*

Proof: Let $G = \mathbb{Z}/N\mathbb{Z}$. Let $x, y, z \in G$. We see that $\chi_x(y + z) = e^{2\pi i x(y+z)/N} = \chi_x(y)\chi_x(z)$ so χ_x is a character of G for each $x \in G$. Moreover, we see that

$(\chi_x \cdot \chi_y)(z) = \chi_x(z)\chi_y(z) = \chi_{x+y}(z)$ so the set of characters is closed under multiplication. Since χ_0 is the trivial character, which is the constant function 1, we deduce that $\hat{G}$ is a group under multiplication of functions and that χ is a homomorphism. In fact we can see that the map is an isomorphism. ∎

Thus for any cyclic group we have that $\hat{G} \cong G$ in a natural way. This extends to the case of any abelian group but the correspondence depends on some choices.

The following theorem can be also seen in [4, Section 3].

Theorem 3.1.16. *For a finite abelian group G,*

$$\hat{G} \cong G \tag{3.1.4}$$

Proof: Let G be a finite abelian group. Then we can express it as $G = G_1 \times \cdots \times G_k$, where each G_i is cyclic.

For each $i \in \{1, \ldots, k\}$, define a map $f_i : \hat{G}_i \to G_i$ via $f(\chi_g) = g$. By Lemma 3.1.15 this is an isomorphism.

Now, all that remains to show is that $\widehat{G_i \times G_j} \cong \hat{G}_i \times \hat{G}_j$. Then the result can be extended to $G = G_1 \times \cdots \times G_k$.

Let χ be a character of $G_i \times G_j$. Let $\chi_i : G_i \to \mathbb{C}^*$ be a map $\chi_i(g) = \chi(g, 1)$. Let $\chi_j : G_j \to \mathbb{C}^*$ be a map $\chi_j(g) = \chi(1, g)$. Both of this maps are homomorphisms. Now note that we can rewrite $(g, g') \in G_i \times G_j$ as $(g, 1)(1, g')$. So we have

$$\chi(g, g') = \chi[(g, 1)(1, g')] = \chi(g, 1)\chi(1, g') = \chi_i(g)\chi_j(g'). \tag{3.1.5}$$

So we have a homomorphism between $\widehat{G_i \times G_j}$ and $\hat{G}_i \times \hat{G}_j$. It is also surjective since the cardinality of $\widehat{G_i \times G_j}$ and $\hat{G}_i \times \hat{G}_j$ is the same. Now to see that it is an isomorphism note that if $\chi_i(g)\chi_j(g') = \chi_i(h)\chi_j(h')$, then $\chi(g, g') = \chi(h, h')$. ∎

For a non-abelian group, $Cl(G) \neq \mathbb{C}^G$, so the set of irreducible characters $\hat{G}$ does not give us a basis for the set of all functions on G, unlike the abelian case. We will see that is a key difference that makes the nonabelian case of the HSP much more difficult. We have an important result, proven in [23, Remarks in Section 2.3 on p.14, 15].

To state it, recall that for each representation $\rho\colon G \to GL(V)$, we can choose a basis B of V and this gives a matrix $\rho_B(g) = (\rho_{ij}(g))_{i,j}$. In fact, we can always choose B so that $\rho_B(g)$ is a unitary matrix. The entries of these matrices define functions from G to $\mathbb{C}$, called the matrix coefficients of ρ with respect to B.

Theorem 3.1.17. *Let G be a finite group. Choose a basis for each irreducible representation ρ of G so that the matrix $M_\rho(g)$ is a unitary. Then the set of all of these matrix coefficients forms an orthogonal basis for $\mathbb{C}^G$.*

Moreover, by Remark after Corollary 3 in [23], it follows that for every irreducible representation ρ of G, the set of all normalized matrix coefficients of $M_\rho(g)$, $\{\sqrt{d_\rho}(\rho, i, j) \mid (\rho, i, j)$ is the ij-th coefficient of the matrix $M_\rho(g)\}$ is an orthonormal basis for $\mathbb{C}^G$.

3.1.2 Quantum computing

The following subsection is based on the Introduction to Quantum Computing course taught in Carleton University by Dr. Jason Crann. The course is based on the well-known textbook by Nielsen and Chuang [19].

Definition 3.1.18. A (finite-dimensional) Hilbert space $\mathcal{H}$ is a finite-dimensional complex inner product space.

Recall that we call a complex vector space V an inner product space when V is equipped with a sesquilinear form $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ satisfying the equations below for any $u, v, w \in V$ and $\lambda, \beta \in \mathbb{C}$.

$$\begin{aligned} \langle u, u\rangle &\geq 0 \\ \langle u, u\rangle &= 0 \text{ if and only if } u = 0 \\ \langle u, \lambda v + \beta w\rangle &= \lambda\langle u, v\rangle + \beta\langle u, w\rangle \\ \langle \lambda v + \beta w, u\rangle &= \overline{\lambda}\langle v, u\rangle + \overline{\beta}\langle w, u\rangle \\ \overline{\langle u, v\rangle} &= \langle v, u\rangle \end{aligned} \tag{3.1.6}$$

Note also that any Hilbert space $\mathcal{H}$ carries a norm given by $||\psi|| = \sqrt{\langle \psi, \psi\rangle}$ which consequently satisfies the equations below for any $\psi, \phi \in V$, and $\lambda \in \mathbb{C}$.

$$||\psi|| = 0 \text{ if and only if } \psi = 0 \tag{3.1.7}$$

$$||\lambda\psi|| = |\lambda|||\psi|| \tag{3.1.8}$$

$$||\psi + \phi|| \leq ||\psi|| + ||\phi|| \tag{3.1.9}$$

Every Hilbert space $\mathcal{H}$ admits an orthonormal basis i.e. an algebraic basis $\{\psi_0, \ldots, \psi_{N-1}\}$ such that $\langle \psi_i, \psi_j\rangle = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{else.} \end{cases}$

Definition 3.1.19. Given two Hilbert spaces $\mathcal{H}, \mathcal{K}$, the space of linear operators from $\mathcal{H}$ to $\mathcal{K}$ is denoted $L(\mathcal{H}, \mathcal{K}) = \{T : \mathcal{H} \to \mathcal{K} | T \text{ is linear }\}$. Now if $\mathcal{K} = \mathbb{C}$, then $L(\mathcal{H}, \mathcal{K}) = \mathcal{H}^*$, the dual of $\mathcal{H}$. The dual space $\mathcal{H}^*$ also called the space of linear functionals on $\mathcal{H}$. Also, if $\mathcal{H} = \mathcal{K}$ then we write just $L(\mathcal{H})$ for $L(\mathcal{H}, \mathcal{K})$.

Suppose that $\mathcal{H}$ is a Hilbert space and $A \in L(\mathcal{H})$. The adjoint of A is the matrix, denoted A^*, which satisfies the equation

$$\langle A^*\phi, \psi\rangle = \langle \phi, A\psi\rangle \tag{3.1.10}$$

for all $\phi, \psi \in \mathcal{H}$. Choose an orthonormal basis of $\mathcal{H}$, and write A as a matrix relative to that basis. It is given simply by the formula $A^* = \bar{A}^T$, where the complex conjugate is taken component-wise.

We will now introduce a special notation that we will be using throughout this chapter, called the "Dirac notation". Using this notation we will denote vectors in $\mathcal{H}$ by "kets", i.e. a column vector ψ becomes $|\psi\rangle$. Dual vectors in $\mathcal{H}^*$ are denoted as "bras". If ψ is a dual vector, we denote it as $\langle\psi|$. The intuition behind this notation is that if $|\psi\rangle$ is a vector in $\mathcal{H}$, then the operator defined by $\phi \mapsto \langle\psi, \phi\rangle$ is a linear function on $\mathcal{H}$, which we denote $\langle\psi|$. Therefore $\langle\psi||\phi\rangle = \langle\psi, \phi\rangle$, a "braket" in $\mathbb{C}$ i.e. the inner product of $|\psi\rangle, |\phi\rangle \in \mathcal{H}$.

Let's look at this notation a little more closely. Fix an orthonormal basis $\{|\psi_0\rangle, \ldots, |\psi_{N-1}\}\rangle$ of $\mathcal{H}$. Then any $|\psi\rangle \in \mathcal{H}$ can be identified with a column vector whose entries are $\langle\psi_i, \psi\rangle = \lambda_i$. Then the dual vector $\langle\psi|$ is a row vector with entries $\overline{\lambda_i}$ i.e. complex conjugates of λ_i.

Example. Let $\mathcal{H} = \mathbb{C}^4$. Let the standard basis of $\mathbb{C}^4, \{e_0, e_1, e_2, e_3\}$, be denoted by $|i\rangle = |e_i\rangle$. Then $|2\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$, and $\langle 0| = \begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$.

Definition 3.1.20. Let $U \in L(\mathcal{H}, \mathcal{H})$ be a linear operator such that $U^*U = I$, where I is the identity matrix. Such linear operator is called a unitary operator.

Example. The Pauli matrices

$$X = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, Y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}, Z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \tag{3.1.11}$$

are all examples of unitary linear operators. For instance $Y^*Y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}\begin{bmatrix}0 & -i\\i & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$.

Example. Let $|\psi\rangle$ be a unit vector in $\mathcal{H}$. An operator $P = |\psi\rangle\langle\psi|$ acting as $|\psi\rangle\langle\psi|(|\phi\rangle) = \underbrace{\langle\psi|\phi\rangle}_{\in\,\mathbb{C}}|\psi\rangle$ is the orthogonal projection onto the span of $|\psi\rangle$. We call it simply a projection. Projection is not a unitary since $P^*P = |\psi\rangle(\langle\psi||\psi\rangle)\langle\psi| = |\psi\rangle\langle\psi|$.

Note that if the set $\{|\psi_0\rangle, \ldots, |\psi_{N-1}\rangle\}$ is an orthonormal basis for $\mathcal{H}$, then the sum of the projections $\sum_{i=0}^{N-1} |\psi_i\rangle\langle\psi_i|$ is the identity matrix, which is unitary.

Definition 3.1.21. Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces. Then the tensor product of $\mathcal{H}, \mathcal{K}$ is defined as $\mathcal{H} \otimes \mathcal{K} = \operatorname{span}\{|\psi\rangle \otimes |\phi\rangle \mid |\psi\rangle \in \mathcal{H}, |\phi\rangle \in \mathcal{K}\}$ subject to the following relations, for all $|\psi_1\rangle, |\phi_1\rangle \in \mathcal{H}$, $|\psi_2\rangle, |\phi_2\rangle \in \mathcal{K}$, and $\lambda \in \mathbb{C}$. Then

$$(|\psi_1\rangle + |\phi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle + |\phi_1\rangle \otimes |\psi_2\rangle \tag{3.1.12}$$

$$|\psi_1\rangle \otimes (|\psi_2\rangle + |\phi_2\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\phi_2\rangle \tag{3.1.13}$$

$$\lambda(|\psi_1\rangle \otimes |\psi_2\rangle) = (\lambda|\psi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes (\lambda|\psi_2\rangle) \tag{3.1.14}$$

Note that later on we might denote tensor of kets as one ket. For example, $|0\rangle \otimes |0\rangle = |00\rangle$. Moreover, note that if $\{|\phi_i\rangle \mid i \in \{1, \dots, N\}\}$ is an orthonormal basis for $\mathcal{H}$ and $\{|\psi_i\rangle \mid i \in \{1, \dots, M\}\}$ is an orthonormal basis for $\mathcal{K}$, then $\{|\phi_i\rangle \otimes |\psi_j\rangle | i \in \{1, \dots, N\}, j \in \{1, \dots, M\}\}$ is the orthonormal basis for $\mathcal{H} \otimes \mathcal{K}$. The inner product on $\mathcal{H} \otimes \mathcal{K}$ is defined by $\langle \psi_1 \otimes \phi_1, \psi_2 \otimes \phi_2 \rangle = \langle \psi_1, \psi_2 \rangle \langle \phi_1, \phi_2 \rangle$.

Let us also take a look at the tensor product of linear operators. Let $T \in \mathcal{L}(\mathcal{H}), S \in \mathcal{L}(\mathcal{K})$. Then there exists a unique operator $T \otimes S \in \mathcal{L}(\mathcal{H} \otimes \mathcal{K})$ satisfying

$$T \otimes S(|\psi\rangle \otimes |\phi\rangle) = T|\psi\rangle \otimes S|\phi\rangle \tag{3.1.15}$$

for any $|\psi\rangle \in \mathcal{H}, |\phi\rangle \in \mathcal{K}$. Importantly, however, just like not every vector in $\mathcal{H} \otimes \mathcal{K}$ is of the form $|\psi\rangle \otimes |\phi\rangle$, not every linear operator in $L(\mathcal{H} \otimes \mathcal{K})$ is of the form $T \otimes S$.

Let us step away from linear algebra for a second. We will now talk about postulates of quantum mechanics.

Definition 3.1.22. Let $\mathcal{H}$ be a Hilbert space. If we associate $\mathcal{H}$ to an isolated physical system, then $\mathcal{H}$ is called a state space. Each physical state of the system is completely described by a unit vector $\psi \in \mathcal{H}$, denoted the state or the state vector.

The following example nicely combine different notions that we have defined above.

Example. Let $\mathcal{H}$ be the state space, and the system is in the state $|\phi\rangle$. Let $U \in L(\mathcal{H})$ be a unitary operator. We define a controlled unitary operator with control set at $|1\rangle$, as $c\text{-}U : \mathbb{C}^2 \otimes \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}$ acting as

$$c\text{-}U(|0\rangle \otimes |\phi\rangle) = |0\rangle \otimes |\phi\rangle, \; c\text{-}U(|1\rangle \otimes |\phi\rangle) = |1\rangle \otimes U|\phi\rangle.$$

In operator form we write $c\text{-}U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$. Note that we can set control to $|0\rangle$ instead, however that would yield a different unitary.

A composite system is one whose state space is the tensor product of the state spaces of the component systems. Given a state $|\phi_i\rangle$ in the ith component system for each i, the resulting state in the composite system is given by $|\phi\rangle = \bigotimes_i |\phi_i\rangle$.

Definition 3.1.23. Let $\mathcal{H} \otimes \mathcal{K}$ be the state space of a system and suppose the system is in state $|\phi\rangle$. We say that $|\phi\rangle$ is entangled if there do not exist states $|\phi_1\rangle \in \mathcal{H}$ and $|\phi_2\rangle \in \mathcal{K}$, such that $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$. Otherwise, we say the state is separable.

Example. Let $\mathcal{H}\otimes\mathcal{K}$ be a state space having orthonormal basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Let $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ be a state vector of the state space. We will now show that $|\phi\rangle$ is entangled by contradiction.

Assume $|\phi\rangle$ is separable. Then there exists $|\phi_1\rangle \in \mathcal{H}$ and $|\phi_2\rangle \in \mathcal{K}$ such that $|\phi_1\rangle \otimes |\phi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Now the vectors $|\phi_1\rangle$ and $|\phi_2\rangle$ can be written using the orthonormal basis. That means that $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) = (a_1|0\rangle + b_1|1\rangle)\otimes(a_2|0\rangle + b_2|1\rangle)$. We can rewrite this expression as $a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + a_2b_2|11\rangle$. For this to equal $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we would need the coefficients to solve

$$a_1a_2 = \frac{1}{\sqrt{2}}, \quad a_1b_2 = 0, \quad b_1a_1 = 0, \quad b_1b_2 = \frac{1}{\sqrt{2}} \tag{3.1.16}$$

which is not possible. Thus, the assumption fails and the state $|\phi\rangle$ is indeed entangled.

Definition 3.1.24. The evolution of a closed quantum system is described by a unitary transformation U i.e. if at time $t = 0$ the state of the system is $|\phi_0\rangle$, then the state of the system at the time $t = 1$ is $U|\phi_0\rangle = |\phi_1\rangle$.

Let $\mathcal{H}$ be a Hilbert space with orthonormal basis $\{|0\rangle, |1\rangle\}$. Let $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Suppose that the system associated to $\mathcal{H}$ is in state $|\psi\rangle$. Then we say that the system is in a superposition of states $|0\rangle$ and $|1\rangle$. If we try to observe the state $|\psi\rangle$ we will observe $|0\rangle$ half of the time and state $|1\rangle$ half of the time.

We now introduce the concept of measuring a quantum system, which is the mathematical analogue of trying to observe the state.

Definition 3.1.25. A quantum measurement of a quantum system $\mathcal{H}$ is a set of operators $\{M_i\} \in \mathcal{L}(\mathcal{H})$, for all $i \in \{1, \ldots, K\}$, satisfying $\sum_{i=1}^{K} {M_i}^* M_i = I$. The collection of these operators is referred to as a measurement system.

The index i refers to the possible measurement outcomes. Let $|\psi\rangle$ be the state describing the system immediately before the measurement, then the probability of outcome i is defined to be

$$p_i = ||M_i|\psi\rangle||^2. \tag{3.1.17}$$

Now assume the outcome i occurred. Then the state describing $\mathcal{H}$ right after the measurement is

$$|\psi_i\rangle = \frac{1}{\sqrt{p_i}} M_i|\psi\rangle \tag{3.1.18}$$

Let us verify that the p_i's can indeed be thought of as probabilities. We have from (3.1.17) that each

$$p_i \geq 0.$$

Moreover, if $|\psi\rangle$ is any state then by the definition of the adjoint and equation (3.1.6) we have

$$\sum_i p_i = \sum_i ||M_i|\psi\rangle||^2 = \sum_i \langle M_i|\psi\rangle, M_i|\psi\rangle\rangle$$
$$= \sum_i \langle \psi | M_i{}^* M_i \psi\rangle = \langle \psi | \sum_i M_i{}^* M_i \psi\rangle = \langle \psi, \psi\rangle = 1.$$

Example. Let $\mathcal{H}$ be a Hilbert space with orthonormal basis $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. We will show that the projection operators of the form $|i\rangle\langle i|$, for $i \in \{0,1,2,3\}$ define a system of measurement operators $M_i = |i\rangle\langle i|$. Note that $M_i{}^* = |i\rangle\langle i| = M_i$. Thus, $M_i{}^* M_i = M_i{}^2 = |i\rangle(\langle i||i\rangle)\langle i| = |i\rangle\langle i| = M_i$. So, the sum $\sum_{i=0}^{3} M_i{}^* M_i = \sum_{i=0}^{3} |i\rangle\langle i| = I$. Suppose that the state before measurement describing the system $\mathcal{H}$ is $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$. Then outcomes $i = 0, 3$ have probability $p_0 = p_3 = 0$ and outcomes $i = 1, 2$ both have probability equal to $\frac{1}{2}$.

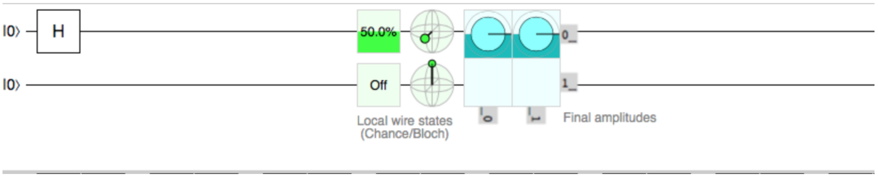
This kind of measurement system is very common. We call it measuring the system relative to the given orthonormal basis.

The last part of the quantum background we need to acquire is circuit-gate formalism. Whenever we will refer to the input of a quantum system, we mean quantum states, and when we refer to gates, we really only mean unitary operators. When we refer to the register what we mean is the chosen component of a system comprising multiple qubits. It is the quantum analog of the classical processor register. And lastly, when we refer to the measurement we mean measurement as a part of the circuit, and note that we can measure each register separately.

Example. The Hadamard gate is a unitary operator H such that $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$, and $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$. Written as a matrix the Hadamard gate is $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, which we can see is a unitary matrix.

It might be helpful for the reader to keep in mind a picture of the quantum circuit. Whenever we are going to be talking about registers, gates and measurement we hope the reader will picture the respective quantum circuit in their head in order to help and understand the results better.

Let $\mathcal{H}$ and $\mathcal{K}$ be two state spaces with bases $\{|0\rangle, |1\rangle\}$. The picture below describes a quantum circuit build using *https://algassert.com/quirk*.

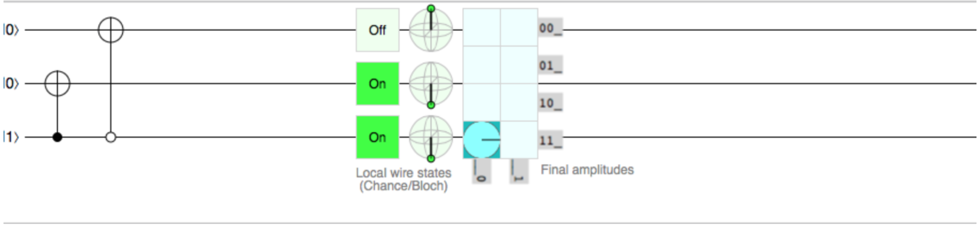


The system $\mathcal{H} \otimes \mathcal{K}$ is depicted using two registers. The input into each of the two registers is $|0\rangle$, so the system is initially in the state $\phi_0 = |00\rangle$. The box in the circuit illustrates that we now apply the Hadamard gate to the first register only, transforming the first component into the state $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The output is the tensor product of the two output registers, which is $|+\rangle \otimes |0\rangle$. Mathematically, we can write this quantum transformation as

$$H \otimes I(|\phi_0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle).$$

Now, if we measure the output relative to the orthonormal basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the probability of measuring $|00\rangle$ is $p_{00} = \frac{1}{2} = p_{10}$, when the probability of measuring $|01\rangle$ is $p_{01} = 0 = p_{11}$.

For this next circuit, assume again that $\mathcal{H}_1, \mathcal{H}_2$ and $\mathcal{H}_3$ are three state spaces with bases $\{|0\rangle, |1\rangle\}$. The picture below form *https://algassert.com/quirk* depicts a quantum circuit of the system $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ using three registers. The first two registers are initialized to the state vector $|0\rangle$, the third one however is set to $|1\rangle$. So the system is in the state $\phi_0 = |001\rangle$.



Now we will apply two controlled Pauli X-gates. Recall, that $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. So the action of X on $|0\rangle$ and $|1\rangle$ is

$$X|0\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle = |1\rangle,$$

and

$$X|1\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)|1\rangle = |0\rangle.$$

The first two connected circles depict a controlled unitary X, with control at $|1\rangle$ being applied to a state $|0\rangle$ in the second register. The state $|1\rangle$ in the third register is a control. We will write the operation on the two registers as

$$c\text{-}U_1 = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

This controlled unitary yields the state in the last two registers $|11\rangle$. The action on the whole system can be written as

$$I \otimes c\text{-}U_1 \otimes I(|0\rangle \otimes |0\rangle \otimes |1\rangle) = |0\rangle \otimes X|0\rangle \otimes 1 = |0\rangle \otimes |1\rangle \otimes |1\rangle = |011\rangle.$$

So the state of the entire system after applying the first controlled X is $|011\rangle$.

The second two connected circles also depict a controlled X-gate. The unitary X in this case is applied to a state in the first register, and the control is set to the third register. Note however, that this time the control is set at $|0\rangle$. In operator form we can write such a controlled unitary as

$$c\text{-}U_2 = |0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes I.$$

The state of the entire system before applying c-U_2 is 011. The action of the unitary is

$$c\text{-}U_2 \otimes I \otimes I(|0\rangle \otimes |1\rangle \otimes |1\rangle) = X|0\rangle \otimes 1 \otimes 1 = |0\rangle \otimes |1\rangle \otimes |1\rangle = |011\rangle.$$

So the state of the system at the end remains $|011\rangle$.

3.2 Quantum Fourier Transform

Now that we have laid the groundwork, we can introduce the main component needed to solve the HSP in a quantum setting, the Quantum Fourier Transform. Note that we will start by defining the standard method of solving HSP over abelian groups using the language of representation theory, however later on we will focus solely on quantum computing and will define the standard method of solving HSP over any general group using the language of quantum computing almost exclusively.

3.2.1 Quantum Fourier Transform: abelian groups

We will now discuss the core result of many quantum algorithms to solve HSP, the Quantum Fourier transform (QFT). The QFT is a unitary transformation obtained as the transformation from one orthonormal basis to another.

Let G be an abelian group of order N. Consider the characteristic function of g, $1_g : G \to \mathbb{C}$, defined via

$$1_g(g') = \begin{cases} 1, & \text{if } g' = g \\ 0, & \text{if } g' \neq g. \end{cases}$$

If $f : G \to \mathbb{C}$ is any function, then

$$f = \sum_{g \in G} f(g) 1_g, \tag{3.2.1}$$

since for any $h \neq g$, we have $f(h) = \sum_{g \in G} f(g) 1_g(h) = f(h) 1_h(h) + \sum_{g \neq h} f(g) \underbrace{1_g(h)}_{=0} = f(h)$.

Therefore $\{1_g \mid g \in G\}$ is a basis for $\mathbb{C}^G$. Let us show that it is orthogonal with respect to the inner product (Definition 3.1.10). For any $t, h \in G$, we have

$$\begin{aligned}\langle 1_t, 1_h \rangle &= \frac{1}{|G|}\sum_{g\in G} 1_t(g) 1_h(g)^* \\ &= \begin{cases} 0, \text{ if } t \neq h \\ \frac{1}{|G|}\sum_{g\in G} 1_t(g)1_t(g)^* = \frac{1}{|G|}1_g(g)\overline{1_g(g)} = \frac{1}{|G|}, \text{ if } t = h. \end{cases}\end{aligned} \tag{3.2.2}$$

We can thus scale each of these basis vectors by $\sqrt{|G|}$ to get an orthonormal basis $B_2 = \{\sqrt{|G|}1_g \mid g \in G\}$.

On the other hand, by Lemma 3.1.14, the set, $\hat{G} = \{\chi_i \mid i \in \{1, \ldots, N\}\}$, forms a basis B_1 for $\mathbb{C}^G$. So any complex valued function f is a linear combination of irreducible characters of G. Since elements of $\hat{G}$ are an orthonormal basis, the coefficients of f relative to the basis are easy to compute using the inner product, yielding the following equation:

$$f = \sum_{j=1}^{N} \langle f, \chi_j \rangle \chi_j.$$

Suppose that $f = 1_g$. Then since $\langle 1_g, \chi_j \rangle = \frac{1}{|G|}\sum_{t\in G} 1_g(t)\chi_j(t)^* = \frac{1}{|G|}(1_g(g)\chi_j(g)^* + \sum_{t\neq g} \underbrace{1_g(t)}_{=0} \chi_j(t)^*) = \frac{1}{|G|}\chi_j(g)^*$, we have

$$\sqrt{|G|}1_g = \sqrt{|G|}\sum_{j=0}^{N-1}\langle 1_g, \chi_j\rangle \chi_j = \frac{1}{\sqrt{|G|}}\sum_{j=0}^{N-1} \chi_j(g)^* \chi_j, \tag{3.2.3}$$

We will now identify each of the bases B_1 and B_2 with the computational basis. We will write $|\chi_l\rangle$ for $|l\rangle$, where $l \in G$. This little remark is useful as later there will be no obvious way to do this mapping.

Define the action of $F_G : \mathcal{H} \to \mathcal{H}$ by the conjugate of (3.2.3):

$$F_G(|g\rangle) = \frac{1}{\sqrt{|G|}}\sum_{l=0}^{N-1} \chi_l(g)|\chi_l\rangle \tag{3.2.4}$$

Then this is a unitary transformation because it maps one orthonormal basis to another. The function F_G can be written as

$$F_G = \frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}\sum_{k=0}^{N-1} \chi_l(k)|\chi_l\rangle\langle k|. \tag{3.2.5}$$

Now consider the special case that $G = C_N$. Then the characters of G were defined in Definition 3.1.7, and are indexed by the elements of G. More precisely,we have $\chi_l(k) = e^{\frac{2\pi ilk}{N}}$ for any $l, k \in G$.

This yields the simplified QFT from [12],

$$F_N|k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}} |l\rangle. \tag{3.2.6}$$

The function F_G in this case is

$$F_G = F_N = \frac{1}{\sqrt{N}} \sum_{l=0,x=0}^{N-1} e^{\frac{2\pi ikl}{N}} |l\rangle\langle k|.$$

Note that so far we have defined an action of the QFT on the orthonormal basis vectors. The action of QFT on any arbitrary state can be defined through its orthonormal basis vectors. Let $|x\rangle$ be an arbitrary state in $\mathcal{H}$, i.e. $|x\rangle = \sum_{j=0}^{N-1} x_j|j\rangle$. Then

$$\begin{aligned} F_N|x\rangle &= F_N \sum_{k=0}^{N-1} x_k|k\rangle \\ &= \sum_{k=0}^{N-1} x_k \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{\frac{2\pi ikl}{N}} |l\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} x_k e^{\frac{2\pi ikl}{N}} |l\rangle \end{aligned} \tag{3.2.7}$$

3.2.2 Quantum Fourier Transform: general groups

Let G be a group. Let $\hat{G}$ be the set of all irreducible representations of G. Recall, that QFT is a change of basis transformation. In case of finite abelian groups, we can relate a conjugacy class to a character, which in turn allows us to identify every element of a group G with a character. When G is a nonabelian group, we can no longer use characters this way. Lemma 3.1.12 tells us that in the general setting the set of all characters of G does not form an orthonormal basis for the space of all complex valued functions on G, but rather for the space of all class functions. It's the set of all matrix coefficients of all irreducible representations of G that forms an orthonormal basis for the space of all complex valued functions on G (Lemma 3.1.17).

For each $\sigma \in \hat{G}$, let d_σ be the dimension of its space V and choose an orthonormal basis $\{|i\rangle \mid 1 \leq i \leq d_\sigma\}$ of V. The resulting matrix coefficients can be described by the formulas $|\sigma, i, j\rangle(g) = \langle i|\sigma(g)|j\rangle$, and they form a basis, B_3, of functions in $\mathbb{C}^G$, as σ runs over $\hat{G}$. Recall from the discussion preceding (3.2.2) that B_2 is another orthonormal basis of $\mathbb{C}^G$. Given $g \in G$, we can write $\sqrt{|G|}1_g$ with respect to this new basis of matrix coefficients as

$$\frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \overline{\sigma(g)_{i,j}} |\sigma, i, j\rangle. \tag{3.2.8}$$

After choosing some bijection between each bases B_2, B_3, and the computational basis, we use this to define the general *Quantum Fourier Transform.*

Definition 3.2.1. Let G be a group. Let $\hat{G}$ be the set of all irreducible representations of G. Then the action of the Quantum Fourier Transform is defined as

$$\mathcal{F}_G(|g\rangle) = \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sigma(g)_{i,j} |\sigma, i, j\rangle. \tag{3.2.9}$$

The function itself we can write as a linear operator

$$\mathcal{F}_G = \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sum_{g \in G} \sigma(g)_{i,j} |\sigma, i, j\rangle\langle g|. \tag{3.2.10}$$

Lemma 3.2.2. *The Quantum Fourier Transform as defined in Definition 3.2.1 is a unitary transformation.*

Proof: Recall, that for a linear operator U to be a unitary it must satisfy $U^*U = I$. That is precisely what we will show with $\mathcal{F}_G$ as in (3.2.10). Before we show that $\mathcal{F}_G$ is a unitary, note that its dual is

$$\mathcal{F}_G{}^* = \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sum_{g \in G} \overline{\sigma(g)_{i,j}} |g\rangle\langle \sigma, i, j|.$$

Then we can compute

$$\begin{aligned}
\mathcal{F}_G{}^*\mathcal{F}_G &= \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sum_{g \in G} \overline{\sigma(g)_{i,j}} |g\rangle\langle \sigma, i, j| \frac{1}{\sqrt{|G|}} \sum_{\rho \in \widehat{G}} \sqrt{d_\rho} \sum_{i',j'=1}^{d_\rho} \sum_{h \in G} \rho(h)_{i',j'} |\rho, i', j'\rangle\langle h| \\
&= \frac{1}{|G|} \sum_{\rho,\sigma \in \widehat{G}} \sqrt{d_\sigma}\sqrt{d_\rho} \sum_{i',j'=1}^{d_\rho} \sum_{i,j=1}^{d_\sigma} \sum_{h,g \in G} \overline{\sigma(g)_{i,j}} \rho(h)_{i',j'} |g\rangle(\langle \sigma, i, j||\rho, i', j'\rangle)\langle h| \\
&= \frac{1}{|G|} \sum_{\sigma \in \widehat{G}} d_\sigma \sum_{i,j=1}^{d_\sigma} \sum_{h,g \in G} \overline{\sigma(g)_{i,j}} \sigma(h)_{i,j} |g\rangle\langle h|
\end{aligned}$$

Now note that $\overline{\sigma(g)_{i,j}} = \sigma(g^{-1})_{j,i}$ since $\sigma(g)$ is a unitary matrix. So

$$\mathcal{F}_G{}^*\mathcal{F}_G = \frac{1}{|G|}\sum_{\sigma\in\widehat{G}} d_\sigma \sum_{j=1}^{d_\sigma}\sum_{h,g\in G}[\sum_{i=1}^{d_\sigma}\sigma(g^{-1})_{j,i}\sigma(h)_{i,j}]|g\rangle\langle h|$$

The sum $\sum_{i,j=1}^{d_\sigma}\sigma(g^{-1})_{j,i}\sigma(h)_{i,j}$ becomes $\sum_{j=1}^{d_\sigma}(\sigma(g^{-1})\sigma(h))_{jj}$ as a matrix product for the entry $(\sigma(g^{-1})\sigma(h))_{jj}$. Since σ is a homomorphism this matrix is $\sigma(g^{-1}h)$. Thus, we have

$$\mathcal{F}_G{}^*\mathcal{F}_G = \frac{1}{|G|}\sum_{\sigma\in\widehat{G}} d_\sigma \sum_{h,g\in G}[\sum_{j=1}^{d_\sigma}\sigma(g^{-1})\sigma(h))_{jj}]|g\rangle\langle h|$$

$$= \frac{1}{|G|}\sum_{\sigma\in\widehat{G}} d_\sigma \sum_{h,g\in G}\chi_\sigma(g^{-1}h)|g\rangle\langle h| \text{ by definition of the trace}$$

$$= \frac{1}{|G|}\sum_{h,g\in G}[\sum_{\sigma\in\widehat{G}} d_\sigma\chi_\sigma(g^{-1}h)]|g\rangle\langle h|$$

Here, $\sum_{\sigma\in\widehat{G}} d_\sigma\chi_\sigma(g^{-1}h) = \chi(g^{-1}h)$ is the character of the regular representation. Since the regular character χ satisfies

$$\chi(g) = \begin{cases} 0, & \text{if } g \neq 1; \\ |G|, & \text{if } g = 1. \end{cases},$$

the coefficient is zero unless $g = h$. So the expression becomes:

$$\frac{|G|}{|G|}\sum_{h\in G}|h\rangle\langle h| = \sum_{h\in G}|h\rangle\langle h| = I.$$

∎

3.3 Coset sampling method

We are now ready to dive into quantum algorithms to solve HSP. One of the most common ways to solve HSPs is the *coset sampling method*, which is often called the *standard method* or *Fourier sampling*. Let us start off with a general set up of the method.

3.3.1 Standard method

Let G be a finite group, and H be a hidden subgroup. Let X be a finite set. Let $f : G \to X$ be the hiding function. Let $\mathcal{H}$ be a Hilbert space spanned by the elements of the set X, and let $\mathcal{G}$ be the Hilbert space spanned by elements indexed by the group G.

Step 1: Prepare two registers, the first in a uniform superposition of the elements of G, the second storing states of $\mathcal{H}$, initially set to $|0\rangle$:

$$|\psi_1\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |0\rangle \in \mathcal{G} \otimes \mathcal{H}.$$

Step 2: Evaluate the function f in the second register. This operation produces an entangled state

$$|\psi_2\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle.$$

Step 3: Measure the second register using measurement system, where each measurement operator is the orthogonal projection onto the span of some orthonormal basis vector of $\mathcal{H}$. We will denote such measurement system as

$$\{M_x = |x\rangle\langle x| \; | x \in X\}.$$

Recall, that when we perform a measurement, we act on the state with the entire measurement system. Then probabilistically one outcome occurs. The probability of the outcome "x" is,

$$\begin{aligned} p_x &= ||I \otimes M_x(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle)||^2 \\ &= ||\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes M_x|f(g)\rangle)||^2 \\ &= ||\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |x\rangle\langle x||f(g)\rangle)||^2 \end{aligned}$$

Since the orthonormal basis vectors of $\mathcal{H}$ are elements of X, which in turn are $f(g)$ for some $g \in G$, we have

$$p_x = ||\frac{1}{\sqrt{|G|}} \sum_{g \in G, f(g)=x} |g\rangle \otimes |x\rangle||^2 = \frac{|H|}{|G|}.$$

Notice that the probability of the outcome "x" is independent of x.

Suppose that the outcome "x" has occurred. Then the state after the measurement is

$$\begin{aligned}
|\phi\rangle &= \frac{1}{\sqrt{p_x}} I \otimes M_x\Big(\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle \otimes |f(g)\rangle\Big) \\
&= \frac{\sqrt{|G|}}{\sqrt{|H|}} \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle \otimes M_x |f(g)\rangle) \\
&= \frac{1}{\sqrt{|H|}} \sum_{g\in G} |g\rangle \otimes |x\rangle\langle x||f(g)\rangle \\
&= \frac{1}{\sqrt{|H|}} \sum_{g\in G, f(g)=x} |g\rangle \otimes |x\rangle;
\end{aligned}$$

The set of elements $g \in G$ such that $f(g) = x$ is one coset of H because the function f is H-periodic. Let us call this coset cH. Then the expression becomes:

$$|\phi\rangle = \frac{1}{\sqrt{|H|}} \sum_{h\in H} |ch\rangle \otimes |x\rangle,$$

where $f(ch) = x$ for all $h \in H$.

This state is no longer entangled since we can write it as a tensor product of two states, namely $\frac{1}{|H|}\sum_{h\in H} |ch\rangle$, and $|f(ch)\rangle$. Since the state is no longer entangled we can discard the second register. The resulting *coset state* is then a uniform superposition of the elements of a coset cH, for some (random) $c \in G$. We abbreviate it as

$$|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h\in H} |ch\rangle \in \mathcal{G}.$$

Step 4: Act on the coset state $|cH\rangle$ to deduce some information about the hidden subgroup H. This can be done either through measurement with respect to elements of G or any other suitable way.

Note that Step 4 requires one to be creative in order to deduce some information about H. Suppose that we simply measure the coset state $|cH\rangle$ with respect to the orthonormal basis of $\mathcal{G}$. In this case measurement operators can be indexed by the elements of G, and have form $M_g = |g\rangle\langle g|$. The probability of observing "g'", where

$g' \in cH$ is

$$\begin{aligned} p_{g'} &= ||M_{g'}|cH\rangle||^2 \\ &= ||\frac{1}{\sqrt{|H|}} \sum_{h \in H} M_{g'}|ch\rangle||^2 \\ &= ||\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g'\rangle\langle g'||ch\rangle \\ &= ||\frac{1}{\sqrt{|H|}}|g'\rangle||^2 = \frac{1}{|H|}. \end{aligned}$$

On the other hand, the probability of observing outcome "g''", where $g'' \notin cH$ is

$$\begin{aligned} p_{g''} &= ||M_{g''}|cH\rangle||^2 \\ &= ||\frac{1}{\sqrt{|H|}} \sum_{h \in H} M_{g''}|ch\rangle||^2 \\ &= ||\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g''\rangle\langle g''||ch\rangle \\ &= 0. \end{aligned}$$

So the outcome of the measurement will always yield an element of the coset cH. However, as an observer, we simply see an element $g' \in G$. Since there is no way for us to link the coset to an element of G chosen uniformly at random, we require at least two elements of the same coset to identify H.

One might think that repeating the procedure will help us identify H. Unfortunately, measuring the coset state will destroy it. So it is highly unlikely that repeating Steps 1–3 will produce two elements of the same coset. Since we only observe elements and are unable to link them to any specific cosets, we need a more clever idea than simply measuring the coset states.

3.3.2 Standard method for finite abelian groups

We will start with the case where $G = C_N$ is a cyclic group generated by g. Let H be the hidden subgroup generated by h. Recall, that when $G = C_N$ the action of the QFT is as in the equation (3.2.6).

After performing Steps 1–3 of the coset sampling method, that yields some coset state $|cH\rangle$. Since G is cyclic, and we know the generators of G and H, the coset $|cH\rangle$ can be expressed as $|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{s=0}^{|H|-1} |c + sh\rangle$.

We will break Step 4 of the standard method into two parts, Step 4a, and Step 4b. These parts are as follows.

Step 4a: Apply $\mathcal{F}_N$ to the coset state $|cH\rangle$.

$$\begin{aligned}
\mathcal{F}_N(|cH\rangle) &= \frac{1}{\sqrt{|G|}} \sum_{l=0,k=0}^{N-1} e^{\frac{2\pi i l k}{N}} |l\rangle\langle k| (\frac{1}{\sqrt{|H|}} \sum_{s=0}^{|H|-1} |c+sh\rangle) \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{l=0,k=0}^{N-1} \sum_{s=0}^{|H|-1} e^{\frac{2\pi i l k}{N}} |l\rangle (\langle k||c+sh\rangle) \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{l=0}^{N-1} \sum_{s=0}^{|H|-1} e^{\frac{2\pi i l(c+sh)}{N}} |l\rangle \text{ by orthogonality} \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{l=0}^{N-1} e^{\frac{2\pi i l c}{N}} |l\rangle (\sum_{s=0}^{|H|-1} e^{\frac{2\pi i s h l}{N}})
\end{aligned}$$

Note that $\sum_{s=0}^{|H|-1} e^{\frac{2\pi i s h l}{N}}$ is nonzero only when $\frac{N}{h} = |H|$ divides l. Not only is it nonzero, we actually have that $\sum_{s=0}^{|H|-1} e^{\frac{2\pi i l h s}{N}} = |H|$. So the equation becomes

$$\mathcal{F}_N(|cH\rangle) = \frac{\sqrt{|H|}}{\sqrt{|G|}} \sum_{l=0}^{N-1} e^{\frac{2\pi i l c}{N}} |l\rangle.$$

Step 4b: Measure $\mathcal{F}_N(|cH\rangle)$ with respect to the orthonormal basis of elements of G. This yields, with certainty, an element $l \in G$, such that l is a multiple of $|H|$.

Now that we have obtained a multiple of $|H|$, we repeat the procedure, in order to deduce $|H|$. Note that the gcd of t successive iterations converges exponentially to $|H|$, and for large N the probability this gcd is equal to $|H|$ is at least $1 - \frac{1}{2^t}$ [7, Lemma 6.1]. Once we have $|H|$, we can easily deduce H.

Now let's focus on the case when G is a finite abelian group of order N. Let $X(H) = \{\chi \in \hat{G} \mid \chi(h) = 1 \forall h \in H\}$. This is the set of characters of G which restrict to the trivial character on H. Recall that for an abelian group G, $\hat{G}$ is a group under multiplication.

Lemma 3.3.1. *If H is a subgroup of G, then $X(H)$ is a subgroup of $\hat{G}$.*

Proof: The trivial character is in $X(H)$. If $\chi, \chi' \in X(H)$, then for all $h \in H$ we have $\chi\chi'(h) = \chi(h)\chi'(h) = 1$ and $\chi(h)^{-1} = 1$ so $X(H)$ is closed under multiplication and inverses. Therefore $X(H)$ is a subgroup of $\hat{G}$. ▮

Now let us prove an important property of $X(H)$.

Lemma 3.3.2. *Let H be a subgroup of a finite abelian group G. Then for any character $\chi \in \hat{G}$ we have*

$$\sum_{h \in H} \chi(h) = \begin{cases} |H| & \text{if } \chi \in X(H); \\ 0, \text{ otherwise.} \end{cases}$$

Proof: Let $\chi \in \hat{G}$. Then $\chi \colon G \to \mathbb{C}^*$ is a homomorphism. Let H be a subgroup of G. Then defining the restriction of χ to H by the formula $\chi|_H(h) = \chi(h)$ for all $h \in H$ gives a homomorphism $\chi|_H \colon H \to \mathbb{C}^*$. Thus $\chi|_H \in \hat{H}$ and by Theorem 3.1.8, $\sum_{h \in H} \chi|_H(h) = 0$ unless $\chi|_H$ is the trivial character of H, that is, unless $\chi \in X(H)$. ▮

Now recall that for an abelian group G, the Quantum Fourier Transform is a map from $\mathcal{G}$ to $\hat{\mathcal{G}}$ given by the formula

$$\mathcal{F}_G = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(g) |\chi\rangle\langle g|.$$

We now use it to extract information from the coset state $|cH\rangle$ obtained in Step 3 of the standard method. If you look at Step 4 of the standard method you will recognize that it does not guarantee that we can find the hidden subgroup H but rather allows us to deduce some sort of information to help us find H. It is now up to us to create an action on the coset state that will yield as much information about H as possible.

The standard method continues after Steps 1–3 as:

Step 4a Apply $\mathcal{F}_G$ to the coset state $|cH\rangle$ to get

$$\begin{aligned}
\mathcal{F}_G(|cH\rangle) &= \frac{1}{\sqrt{|G|}} \sum_{g\in G} \sum_{\chi\in\hat{G}} \chi(g)|\chi\rangle\langle g| \left(\frac{1}{\sqrt{|H|}} \sum_{h\in H} |ch\rangle \right) \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{g\in G} \sum_{\chi\in\hat{G}} \sum_{h\in H} \chi(g)|\chi\rangle\langle g||ch\rangle \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{\chi\in\hat{G}} \sum_{h\in H} \chi(ch)|\chi\rangle \quad \text{by orthogonality} \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{\chi\in\hat{G}} \sum_{h\in H} \chi(c)\chi(h)|\chi\rangle \quad \text{since } \chi \text{ is a homomorphism} \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{\chi\in\hat{G}} \chi(c) \left(\sum_{h\in H} \chi(h) \right) |\chi\rangle \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{\chi\in X(H)} \chi(c)\,(|H|)\,|\chi\rangle \quad \text{by Lemma 3.3.2} \\
&= \frac{\sqrt{|H|}}{\sqrt{|G|}} \sum_{\chi\in X(H)} \chi(c)|\chi\rangle
\end{aligned}$$

Step 4b Measure $\mathcal{F}_G(|cH\rangle)$ with respect to the basis $|\chi\rangle$ of $\hat{\mathcal{G}}$. This yields, with certainty, an element χ of $X(H)$.

Performing Steps 1–4 sufficiently many times will give us a generating set for the group $X(H)$.

Lemma 3.3.3. *Let H be a subgroup of G. Then*

$$H = \{g \in G \mid \chi(g) = 1 \forall \chi \in X(H)\}.$$

Proof: Let H be a subgroup of G and let $X(H) = \{\chi \in \hat{G} \mid \chi(h) = 1 \forall h \in H\}$. Let $K = \{g \in G \mid \chi(g) = 1 \forall \chi \in X(H)\}$. Then by definition we have $H \subseteq K$.

Since G is abelian, H is a normal subgroup and the group G/H is also abelian. Its group of characters has $|G|/|H|$ elements. We claim it is isomorphic to $X(H)$. Namely, given $\chi \in X(H)$ we can define $\overline{\chi} \in \widehat{G/H}$ by $\overline{\chi}(gH) = \chi(g)$, for any $g \in G$, since the characters in $X(H)$ are constant on the cosets of H in G. Conversely, given a character $\overline{\chi} \in \widehat{G/H}$, the same formula defines a character χ of G that is trivial on H.

Therefore $X(H)$ has $|G|/|H|$ elements. If $H \subsetneq K$, then the same argument would give that $X(H)$ has $|G|/|K|$ elements. Therefore $|H| = |K|$, and so $H = K$. ∎

Therefore, once we have identified a generating set for $X(H)$, we will recover H using Lemma 3.3.3. That is, if we have found $\chi_1, \cdots, \chi_l$ elements of $X(H)$ then we have

$$H \subseteq \ker(\chi_1) \cap \ker(\chi_2) \cap \cdots \cap \ker(\chi_l)$$

and we will have equality if $\{\chi_1, \cdots, \chi_l\}$ generates $X(H)$.

In practice, we should use Theorem 3.1.16 to parametrize $\hat{G}$ with a convenient basis, so that we can identify H from $X(H)$ as efficiently as in the cyclic case, and implement the QFT efficiently as well.

3.3.3 Standard method for general groups

Let G be a group. Let H be the hidden subgroup. The first three steps of the standard method to solve the HSP over general group G is the same as the standard method over finite abelian groups. Step 4 can be broken down into two parts, Step 4a, and Step 4b. These two parts are as follows.

Step 4a: Apply the Quantum Fourier Transform as defined in 3.2.1 to a coset state $|g'H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |g'h\rangle$:

$$\begin{aligned}
\mathcal{F}_G(|g'H\rangle) &= \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sum_{g \in G} \sigma(g)_{i,j} |\sigma, i, j\rangle \langle g| (\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g'h\rangle) \\
&= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sum_{g \in G} \sum_{h \in H} \sigma(g)_{i,j} |\sigma, i, j\rangle (\langle g||g'h\rangle) \\
&= \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \widehat{G}} \sqrt{d_\sigma} \sum_{i,j=1}^{d_\sigma} \sum_{h \in H} \sigma(g'h)_{i,j} |\sigma, i, j\rangle \text{ by orthogonality.}
\end{aligned}$$

Step 5b: Perform a measurement or some other operation to observe a classical piece of information that will either yield H or help unveil H.

In case of abelian groups we have performed measurements to learn some information about H. In case of general group, note that after performing measurement we will observe some "σ, i, j", which is a pair of an irreducible representation $\sigma \in \hat{G}$ and one of its matrix coordinates (i, j). Unfortunately, this information might not be enough to learn H unless there has been a clever choice of basis for the matrix $\sigma(g)$, or there is an algorithm that will efficiently deduce H from "σ, i, j".

Chapter 4

Dihedral HSP

The eventual goal of this master thesis is to study possible solutions to the HSP over dihedral group. The dihedral group, being a "nicer" non-abelian group, is the ideal next step after the finite abelian groups to study HSP. Despite being a relatively well understood and well behaved group, there has been little success efficiently solving the HSP over the dihedral group. The goal of these sections is to help the reader understand the challenges in solving the HSP over dihedral groups and to see the beauty of the problem over the dihedral groups.

4.1 Dihedral group

Recall, that a dihedral group D_{2n} is a group of all rotations and reflections of an n-gon. We denote it $D_{2n} = \langle r, s \mid r^n = s^2 = rsrs = 1\rangle$. As a set we denote $D_{2n} = \{r^k, r^k s \mid 0 \leq k < n\}$.

Alternately, by sending $r^\ell s^\varepsilon$ to the pair (ℓ, ε), we can identify D_{2n} with the semi-direct product of cyclic groups $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, with operation $(\ell_1, \varepsilon_1) \cdot (\ell_2, \varepsilon_2) = (\ell_1 + (-1)^{\varepsilon_2}\ell_2, \varepsilon_1 + \varepsilon_2)$, for $\ell_1, \ell_2 \in \mathbb{Z}/n\mathbb{Z}$ and $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}/2\mathbb{Z}$. The image $C_n \subset D_{2n}$ of $\mathbb{Z}/n\mathbb{Z}$ under this map is the group of rotations.

Recall, that by Lemma 2.4.5 the dihedral group D_{2n} has

$$\tau(n) + \sigma(n)$$

subgroups, where $\tau(n)$ is the number of divisors of n and $\sigma(n)$ is the sum of the divisors of n. By Lemma 2.4.2 these subgroups can be enumerated as follows. For each divisor d of n, the subgroup $\langle r^d\rangle$ generated by r^d is a cyclic subgroup of order $\frac{n}{d}$. Further, for each divisor d of n and for each $0 \leq e < d$, the subgroup $\langle r^d, r^e s\rangle$ is a dihedral subgroup of order $\frac{2n}{d}$. Of particular interest is the case $d = n$; the corresponding subgroups $\langle r^e s\rangle$, for $0 \leq e < n$ are the reflection groups of order 2. These subgroups have many cosets, which makes the HSP with the hidden subgroups being $\langle r^e s\rangle$, for $0 \leq e < n$ especially challenging.

Lemma 4.1.1. *Let $G = D_{2n}$ be a dihedral group. The total number of conjugacy classes is $\frac{n}{2} + 3$, when n is even, and $\frac{n+3}{2}$ if n is odd.*

Proof: Let $G = D_{2n}$. Recall, that S is a conjugacy class of s if $S = \{g^{-1}sg \mid g \in G\}$. Let us first consider conjugacy classes of rotations. We conjugate r^i by r^j and r^i by $r^j s$, for any $0 \leq i, j < n$. Thus, we get the following classes:

$$\{r^{-j}(r^i)r^j, (r^j s)^{-1}(r^i)r^j s \mid 0 \leq j < n\} = \{r^i, r^{-i}\},$$

for all $i \in \{0, \ldots, k\}$. When n is even, $k = \frac{n}{2}$. When n is odd $k = \frac{n-1}{2}$.

Now we consider conjugacy classes of reflections. We conjugate $r^i s$ by r^j and $r^i s$ by $r^j s$, for any $0 \leq i, j < n$. Thus, we get the following classes:

$$\{r^{-j}(r^i s)r^j, (r^j s)^{-1}(r^i s)r^j s\} = \{r^{i-2j}s, r^{2j-i}s\} = \{r^l s\},$$

for some $0 \leq l < n$. Now note that if l is odd, $r^l s$ is conjugate to $r^k s$ for any odd $0 < k < n$. It is also true that $r^l s$ is a conjugate to $r^k s$ for any $0 \leq k < n$ if both l and k are even. If n is even we get precisely these two conjugacy classes. If n is odd we get a single conjugacy class.

The total number of conjugacy classes of rotations when n is even is $\frac{n}{2} + 1$, and $\frac{n+1}{2}$ when n is odd. The total number of conjugacy classes of reflections when n is even is 2, and 1 when n is odd. Thus, the result of the lemma follows. ∎

Now that we know the conjugacy classes of D_{2n} we can refer to the Corollary 3.1.13 and determine the irreducible representations of D_{2n}. We will first consider the case when n is even. Note that there are $\frac{n}{2} + 3$ irreducible characters by Corollary 3.1.13. Each distinct character is associated to an irreducible representation. Thus, there are $\frac{n}{2} + 3$ irreducible representations when n is even.

We will first calculate one-dimensional representations by identifying ± 1 to r and s in all possible ways. We can see that one-dimensional representations include the trivial representation ρ and the sign representation τ, given on elements $r^\ell s^\varepsilon \in D_{2n}$ by

$$\rho(r^\ell s^\varepsilon) = 1, \quad \text{and} \quad \tau(r^\ell s^\varepsilon) = (-1)^\varepsilon. \tag{4.1.1}$$

as well as two more one-dimensional representations, θ and ω, given on elements $r^\ell s^\varepsilon \in D_{2n}$ by

$$\theta(r^\ell s^\varepsilon) = (-1)^\ell \quad \text{and} \quad \omega(r^\ell s^\varepsilon) = (-1)^{\ell+\varepsilon}. \tag{4.1.2}$$

Ergo, there are 4 one-dimensional representations when n is even.

Setting $\xi = e^{2\pi i/n}$, the two-dimensional irreducible representations σ_k, for $1 \leq k \leq (n-2)/2$, are given on the elements of D_{2n} by the complex unitary matrices

$$\sigma_k(r^\ell) = \begin{bmatrix} \xi^{kl} & 0 \\ 0 & \xi^{-kl} \end{bmatrix}, \quad \text{and} \quad \sigma_k(r^l s) = \begin{bmatrix} 0 & \xi^{kl} \\ \xi^{-kl} & 0 \end{bmatrix}. \tag{4.1.3}$$

It still remains to determine irreducible representations of D_{2n} when n is odd. There are 2 one-dimensional representations. We can conclude that from identifying ± 1 to r and s in all possible ways. The representations are the trivial representation ρ and the sign representation τ, given on elements $r^\ell s^\varepsilon \in D_{2n}$ by

$$\rho(r^\ell s^\varepsilon) = 1, \quad \text{and} \quad \tau(r^\ell s^\varepsilon) = (-1)^\varepsilon. \tag{4.1.4}$$

The two-dimensional representations are defined by setting $\xi = e^{2\pi i/n}$, the two-dimensional irreducible representations σ_k, for $1 \leq k \leq (n-1)/2$, are given on the elements of D_{2n} by the complex unitary matrices

$$\sigma_k(r^\ell) = \begin{bmatrix} \xi^{kl} & 0 \\ 0 & \xi^{-kl} \end{bmatrix}, \quad \text{and} \quad \sigma_k(r^l s) = \begin{bmatrix} 0 & \xi^{kl} \\ \xi^{-kl} & 0 \end{bmatrix}. \tag{4.1.5}$$

4.2 Standard method

We have described the standard method to solve the HSP over general groups in Section 3.3.3. We will now use this theory and apply it to the special case, when $G = D_{2n}$.

4.2.1 Dihedral Standard Method

Let H be a subgroup of $G = D_{2n}$ hidden by a function $f\colon G \to X$. Restricting f to the rotation subgroup C_n induces a map $f'\colon C_n \to X$ hiding $K = H \cap C_n$ as in Lemma 2.4.12. Using standard method for finite abelian groups with $G = C_n$, hidden subgroup K and hiding function f' efficiently identifies K.

Lemma 4.2.1. *Let $G = D_{2n}$. Let H be the hidden subgroup. Let $K = H \cap C_n$. We may without loss of generality from now on assume that H is either trivial, or of the form $\langle r^\ell s\rangle$ for some $0 \leq \ell < n$.*

Proof: Let $G = D_{2n}$. Let H be the hidden subgroup. Let $K = H \cap C_n$. Suppose we know that $K = \langle r^{n/d}\rangle$, for some positive divisor $d|n$; then by our classification of subgroups of D_{2n}, either $H = \langle r^{n/d}\rangle$ or $H = \langle r^{n/d}, r^\ell s\rangle$ for some $0 \leq \ell < n/d$.

Note that K is a normal subgroup of G, so we may form the quotient group $\overline{G} = G/K$. The quotient is generated by $\overline{r} = rK$ and $\overline{s} = sK$, where $\overline{r}$ is a rotation now of order n/d since $r^{n/d}K = K$ and $\overline{s}$ is still a reflection, so $\overline{G} \cong D_{2n/d}$. Since f is constant on each coset of K in G, it factors through to a well-defined function $\overline{f}\colon \overline{G} \to X$ by the formula $\overline{f}(gK) = f(g)$ for all $gK \in G/K$. The new function $\overline{f}$ hides the subgroup H/K. If $H = K$ then this is the trivial group, and otherwise, $H/K = \langle \overline{r}^\ell \overline{s}\rangle$, one of the two-element reflection subgroups. We have thus argued the following lemma.

∎

Our goal remains to find H. A first promising direction is to apply the standard method to D_{2n}. Steps 1 to 3 are the same, and if $H = \langle r^\ell s\rangle$ then they result in a coset state of the form

$$|r^m H\rangle = |r^{m+\ell} sH\rangle = \frac{1}{\sqrt{2}}\left(|r^m\rangle + |r^{m+\ell}s\rangle\right),$$

for some random $0 \leq m < n$. In this case, Steps 4 and 5 are as follows:

Step 4: Apply the Quantum Fourier Transformation (3.2.9) to a coset state $|r^m H\rangle$:

$$\begin{aligned}\mathcal{F}_G(|r^m H\rangle) &= \frac{1}{\sqrt{|G|}}\sum_{\sigma\in\widehat{G}}\sqrt{d_\sigma}\sum_{i,j=1}^{d_\sigma}\sum_{g\in G}\sigma(g)_{i,j}|\sigma,i,j\rangle\langle g|(\frac{1}{\sqrt{2}}(|r^m\rangle + |r^{m+\ell}s\rangle))\\ &= \frac{1}{\sqrt{|G|}}\frac{1}{\sqrt{2}}\sum_{\sigma\in\widehat{G}}\sqrt{d_\sigma}\sum_{i,j=1}^{d_\sigma}\sigma(r^m)_{i,j} + \sigma(r^{m+\ell}s)_{i,j}|\sigma,i,j\rangle\\ &= \frac{1}{2\sqrt{n}}\sum_{\sigma\in\widehat{G}}\sqrt{d_\sigma}\sum_{i,j=1}^{d_\sigma}\left(\sigma(r^m)_{i,j}|\sigma,i,j\rangle + \sigma(r^{m+\ell}s)_{i,j}|\sigma,i,j\rangle\right).\end{aligned}$$

Step 5: Perform a measurement to observe some $|\sigma, i, j\rangle$, which is the pair of an irreducible representation $\sigma \in \widehat{G}$ and one of its matrix coordinates (i, j).

This time, there is much less simplification. Using the formulas 4.1.5, 4.1.4 and 4.1.2, we can abbreviate $|\sigma, i, j\rangle = |\sigma\rangle$ if $d_\sigma = 1$, and $|\sigma_k, i, j\rangle = |k, i, j\rangle$. To include all cases, set $\delta_a = 1$ if a is even and $\delta_a = 0$ if a is odd. Then we have

$$\begin{aligned}\mathcal{F}_G(|r^m H\rangle) = &\frac{1}{\sqrt{n}}\left(|\rho\rangle + \delta_n\delta_\ell(-1)^m|\theta\rangle + \delta_n\delta_{\ell+1}(-1)^m|\omega\rangle\right) + \\ &+ \frac{1}{\sqrt{2n}}\sum_{k=1}^{(n-1)/2}\left(\xi^{km}|k,1,1\rangle + \xi^{-km}|k,2,2\rangle + \xi^{k(m+\ell)}|k,1,2\rangle + \xi^{-k(m+\ell)}|k,2,1\rangle\right).\end{aligned} \tag{4.2.1}$$

In [9], M Grigni *et. al.* point out that the success of the standard method depends on the amount of statistical information about H present in the probability distribution of the measurement results in Step 5. Here, if we perform a measurment on (4.2.1) with respect to our given choice of bases, then the result is independent of the choice of coset $|r^m H\rangle$. Taking the norm-squared of each of the coefficients in (4.2.1) gives the following probability distribution:

$$P_H(|\sigma,i,j\rangle) = \begin{cases}\frac{1}{2n} & \text{if } \sigma = \sigma_k,\ 0 < k < n/2;\\ \frac{1}{n} & \text{if } \sigma = \rho\text{; or } \sigma = \theta \text{ and } \ell \text{ is even; or } \sigma = \omega \text{ and } \ell \text{ is odd;}\\ 0 & \text{otherwise.}\end{cases}$$

On the other hand, if $H = \{1\}$ is the trivial subgroup, then cosets are singletons and the result of Step 5 is simply the formula (3.2.9). In this case, the probability distribution of measurement outcomes depends on whether the coset is a rotation or a reflection. Writing the conditional probability as $P_H(\text{outcome}|\text{coset})$, we have

$$P_{\{1\}}(|\sigma, i, j\rangle \mid |r^m H\rangle) = \begin{cases} \frac{1}{n} & \text{if } \sigma = \sigma_k,\ 0 < k < n/2 \text{ and } i = j; \\ \frac{1}{2n} & \text{if } \sigma \text{ is one-dimensional;} \\ 0 & \text{otherwise.} \end{cases}$$

for any rotation r^m whereas for any reflection $r^m s$ we have

$$P_{\{1\}}(|\sigma, i, j\rangle \mid |r^m sH\rangle) = \begin{cases} \frac{1}{n} & \text{if } \sigma = \sigma_k,\ 0 < k < n/2 \text{ and } i \neq j; \\ \frac{1}{2n} & \text{if } \sigma \text{ is one-dimensional;} \\ 0 & \text{otherwise.} \end{cases}$$

However, as we cannot know the outcome of Step 3, we can at best observe the average of these two distributions, which we call $P_{\{1\}}$; it is the uniform distribution on $\widehat{G}$.

We observe that the probability distribution of the measurement outcomes of the standard method can provide some partial information about the hidden subgroup. We observe that the probability distribution $P_{\{1\}}$ is distinguishable from the distributions P_H for the reflection subgroups on the 1-dimensional representations; for example, if the outcome of a measurement in Step 5 is τ, then we may conclude $H = \{1\}$. Thus, it is possible to deduce order of the hidden subgroup H by observing the probability distribution of the measurement outcomes of the standard method.

Suppose now that n is even and $H = \langle r^\ell s\rangle$, for some $\ell \in \{0, \ldots, n-1\}$. Then the probability distribution of the measurement outcomes of the standard method reveals the parity of ℓ. That is, if ℓ is even, then $P_H(\omega, 1, 1) = 0$, and if ℓ is odd, then $P_H(\theta, 1, 1) = 0$. So it would be enough to observe θ or ω to conclude the parity of ℓ.

Unfortunately, as per the argument in [9], the standard method cannot distinguish between subgroups of the same order if n is odd, and contains no information beyond the parity of ℓ if n is even. We return to this thought in Section 4.3.

4.2.2 Effect of change of basis on the standard method

The choice of basis with respect to which one writes the two-dimensional representations σ_k defines the measurement basis in Step 5, and thus the probability distribution of the outcomes. Thus one tactic would be to find special basis for the irreducible representations of G that produce a probability distribution of measurement results that conclusively determines H.

So let $U = \begin{bmatrix} v_1 & u_1 \\ v_2 & u_2 \end{bmatrix}$ be a unitary matrix; its columns are an orthonormal basis for $\mathbb{C}^2$ and the representation σ_k^U with respect to this new basis has matrix form $U^\dagger \sigma_k U$. Note, however, that we would like the unitary U to be easily implementable. This way, it will not jeopardize the efficiency of the algorithm. Explicitly, for each $0 \le \ell < n$ we have

$$\sigma_k^U(r^m) = \begin{bmatrix} v_1\overline{v_1}\xi^{km} + v_2\overline{v_2}\xi^{-km} & u_1\overline{v_1}\xi^{km} + u_2\overline{v_2}\xi^{-km} \\ v_1\overline{u_1}\xi^{km} + v_2\overline{u_2}\xi^{-km} & u_1\overline{u_1}\xi^{km} + u_2\overline{u_2}\xi^{-km} \end{bmatrix} \tag{4.2.2}$$

and

$$\sigma_k^U(r^m s) = \begin{bmatrix} v_1\overline{v_2}\xi^{-km} + v_2\overline{v_1}\xi^{km} & u_1\overline{v_2}\xi^{-km} + u_2\overline{v_1}\xi^{km} \\ v_1\overline{u_2}\xi^{-km} + v_2\overline{u_1}\xi^{km} & u_1\overline{u_2}\xi^{-km} + u_2\overline{u_1}\xi^{km} \end{bmatrix}. \tag{4.2.3}$$

In fact, we could choose a different orthonormal basis for each two-dimensional irreducible representation of G, depending in some way on the parameter k.

For each such U and k, this change of basis changes the conditional probabilities $P_H(|\sigma_k^U, i, j\rangle \mid |r^m H\rangle)$, for $1 \le i, j \le 2$, but leaves all others unchanged. Thus, let us suppose as in the previous section that the hidden subgroup is $H = \langle r^\ell s\rangle$, and that the coset state after Step 3 is $|r^m H\rangle$. Using the formula

$$P_H(|\sigma_k^U, i, j\rangle \mid |r^m H\rangle) = \frac{1}{2n}\left|\sigma_k^U(r^m)_{i,j} + \sigma_k^U(r^{m+\ell}s)_{i,j}\right|^2,$$

we obtain the new conditional probabilities:

$$\begin{aligned}
P_H(|\sigma_k^U, 1, 1\rangle \mid |r^m H\rangle) &= \frac{1}{|G|}\left|v_1\overline{v_1}\xi^{km} + v_2\overline{v_2}\xi^{-km} + v_1\overline{v_2}\xi^{-k(m+\ell)} + v_2\overline{v_1}\xi^{k(m+\ell)}\right|^2 \\
P_H(|\sigma_k^U, 1, 2\rangle \mid |r^m H\rangle) &= \frac{1}{|G|}\left|u_1\overline{v_1}\xi^{km} + u_2\overline{v_2}\xi^{-km} + u_1\overline{v_2}\xi^{-k(m+\ell)} + u_2\overline{v_1}\xi^{k(m+\ell)}\right|^2 \\
P_H(|\sigma_k^U, 2, 1\rangle \mid |r^m H\rangle) &= \frac{1}{|G|}\left|v_1\overline{u_1}\xi^{km} + v_2\overline{u_2}\xi^{-km} + v_1\overline{u_2}\xi^{-k(m+\ell)} + v_2\overline{u_1}\xi^{k(m+\ell)}\right|^2 \\
P_H(|\sigma_k^U, 2, 2\rangle \mid |r^m H\rangle) &= \frac{1}{|G|}\left|u_1\overline{u_1}\xi^{km} + u_2\overline{u_2}\xi^{-km} + u_1\overline{u_2}\xi^{-k(m+\ell)} + u_2\overline{u_1}\xi^{k(m+\ell)}\right|^2.
\end{aligned}$$

However, since it is not possible to know the coset state without destroying it after the measurement, we now take the average of these over all cosets $|r^m H\rangle$ to deduce the probability distribution of the standard method in this case. To do so, note that the columns of U have length 1, and that since $0 < k < n/2$, $\sum_{m=0}^{n-1}\xi^{km} = \sum_{m=0}^{n-1}\xi^{2km} = 0$. With some patience we deduce that for $i = 1, 2$:

$$\begin{aligned}
P_H(|\sigma_k^U, i, 1\rangle) &= \frac{1}{|G|}\left|v_1 + v_2\xi^{k\ell}\right|^2 \qquad (4.2.4) \\
P_H(|\sigma_k^U, i, 2\rangle) &= \frac{1}{|G|}\left|u_1 + u_2\xi^{k\ell}\right|^2
\end{aligned}$$

Note that their sum is $4/|G|$, as required, since $(v_1 + v_2\xi^{k\ell}, u_1 + u_2\xi^{k\ell}) = (1, \xi^{k\ell})U$.

Consequently, it is possible to manipulate the choice of bases on the two-dimensional representations so that the probability distribution acts as a signature from which the value of ℓ can be read.

We note, however, that characterizing such a probability distribution directly by empirical methods is exponential in $\log |G|$. For example, an advantageous choice would, for each σ_k, $0 < k < n/2$, be the basis given by

$$U_k = \frac{1}{\sqrt{2}} \begin{pmatrix} -\xi^{k^2} & 1 \\ 1 & \xi^{-k^2} \end{pmatrix}.$$

Then we have $v_1 + v_2\xi^{k\ell} = 0$ if $\ell \equiv k \bmod n/\gcd(k,n)$ and $u_1 + u_2\xi^{k\ell} = 0$ if $\ell \equiv -k \bmod n/\gcd(k,n)$. Each measurement would, by demonstrating the non-vanishing of one of the terms in (4.2.4), eliminate at least one choice of H. However, given the additional work to creating these unitary transformations U_k, this is not even on par with simply querying the oracle f on each reflection.

4.3 Greg Kuperberg's algorithm with $n = 2^m$

Using a clever twist on the standard method, and exploiting its ability to distinguish the parity of ℓ, where $H = \langle r^\ell s \rangle$ is the hidden subgroup, Greg Kuperberg in [14] was able to determine the reflection subgroup using only a subexponential number of queries. The original algorithm, which we summarize here, finds H in $G = D_{2n}$ with time and query complexity $2^{O(\sqrt{\log n})}$, and requires $2^{O(\sqrt{\log n})}$ quantum space [14]. It was later improved in [15], [21].

The idea of the algorithm presented by Greg Kuperberg is to"trap" the hidden subgroup by finding smaller and smaller dihedral subgroups of G containing H until only the hidden subgroup remains. Greg Kuperberg showed that this is possible if the parity of the hidden slope of the reflection is known and the algorithm is repeated a few times until the hidden subgroup H is discovered.

For the presentation of the algorithm, we choose $n = 2^m$ and suppose $H = \langle r^\ell s \rangle$ for some $\ell \in \mathbb{Z}/n\mathbb{Z}$. To simplify notation we identify D_{2n} with $\mathbb{Z}_n \rtimes \mathbb{Z}_2$. Let $\mathcal{H}_1$ be a Hilbert space spanned by the elements indexed by the group $\mathbb{Z}/n\mathbb{Z}$, and let $\mathcal{H}_2$ be the Hilbert space spanned by elements indexed by the group $\mathbb{Z}/2\mathbb{Z}$, so that we represent $|r^a s^b\rangle$ as the state $|a\rangle|b\rangle$.

The algorithm starts with Steps 1–3 of the standard method, yielding a coset state

$$|r^a H\rangle = \frac{1}{\sqrt{2}}(|a\rangle|0\rangle + |a + \ell\rangle|1\rangle).$$

Now, in Step 4, apply the abelian QFT (3.2.4) to only the first register (which contains the group C_n, and corresponds to hiding $H \cap C_n = \{1\}$). The resulting state is thus

$$\begin{aligned}
&\mathcal{F}_n \otimes I|r^aH\rangle \\
&\qquad = \mathcal{F}_n \otimes I(\frac{1}{\sqrt{2}}(|a\rangle|0\rangle + |a+l\rangle|1\rangle)) \\
&\qquad = \frac{1}{\sqrt{2}}(\mathcal{F}_n|a\rangle \otimes |0\rangle + \mathcal{F}_n|a+l\rangle \otimes |1\rangle) \\
&\qquad = \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{n}}\sum_{l,m\in\mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi ilm}{n}}|l\rangle\langle m|a\rangle \otimes |0\rangle + \frac{1}{\sqrt{n}}\sum_{s,t\in\mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi ist}{n}}|s\rangle\langle t|a+l\rangle \otimes |1\rangle) \\
&\qquad = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{n}}(\sum_{l\in\mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi ila}{n}}|l\rangle \otimes |0\rangle + \sum_{s\in\mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi is(a+l)}{n}}|s\rangle \otimes |1\rangle).
\end{aligned}$$

Measure the first register with respect to the orthonormal basis, obtaining a uniformly random outcome k from $\mathbb{Z}/n\mathbb{Z}$. Discard the register, retaining the outcome. Recall that $\xi = e^{\frac{2\pi i}{n}}$. The resulting state in the second register is of the form

$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(\xi^{ka}|0\rangle + \xi^{k(a+\ell)}|1\rangle) = \frac{\xi^{ka}}{\sqrt{2}}(|0\rangle + \xi^{k\ell}|1\rangle). \tag{4.3.1}$$

We note that if $k = n/2 = 2^{m-1}$, then up to global phase (which we henceforth ignore), $|\psi_k\rangle = |+\rangle$ if ℓ is even, and $|\psi_k\rangle = |-\rangle$ if ℓ is odd. Therefore measuring $|\psi_{2^{m-1}}\rangle$ with respect to the basis $\{|+\rangle, |-\rangle\}$ reveals the parity of ℓ.

The final step is to inductively find H: set $R = r^2$. If ℓ is even, then $H = \langle R^{\ell/2}s\rangle$ lies in the index-two dihedral subgroup $\langle R, s\rangle$; if ℓ is odd, set also $S = rs$, and then $H = \langle R^{(\ell-1)/2}S\rangle \subset \langle R, S\rangle$. Iterating this process traps H in $\log(n)$ steps.

Therefore we focus on the parity-finding part of the algorithm.

The key observations are the following. Given states $|\psi_k\rangle, |\psi_l\rangle$, for arbitrary $k, l \in \mathbb{Z}/n\mathbb{Z}$, their tensor product (up to a global phase) is the state

$$|\psi_k\rangle|\psi_l\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + \xi^{k\ell}|1\rangle|0\rangle + \xi^{l\ell}|0\rangle|1\rangle + \xi^{(k+l)\ell}|1\rangle|1\rangle).$$

Apply the controlled X gate, with control set at "1" int he first register, to obtain the new state

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + \xi^{k\ell}|1\rangle|1\rangle + \xi^{l\ell}|0\rangle|1\rangle + \xi^{(k+l)\ell}|1\rangle|0\rangle)$$

and then measure the second register with respect to the orthonormal basis, with outcome p. The resulting state in the first register is then, up to global phase

$$\frac{1}{\sqrt{2}}(|0\rangle + \xi^{(k+(-1)^pl)\ell}|1\rangle) = |\psi_{k+(-1)^pl}\rangle.$$

Now recall that the 2-adic norm of an integer k is $|k|_2 = 2^{-\mathrm{val}(k)}$, when $\mathrm{val}(k)$ is the largest power of 2 dividing k; thus 1 is large and $n/2 = 2^{m-1}$ is small. This norm is an ultrametric, meaning $|k \pm l|_2 \leq \max\{|k|_2, |l|_2\}$ for all $k, l \in \mathbb{Z}/n\mathbb{Z}$. The algorithm seeks to iterate the above steps such that each time, one of $k+l$ or $k-l$ is always strictly closer to $n/2$ in the 2-adic norm.

The algorithm goes as follows:

1. Generate $3 * 8^{\lceil\sqrt{m-1}\rceil}$ states $|\psi_k\rangle$ at random, and store these in a list L_0.

2. Suppose now $1 \leq i < \sqrt{m-1}$, and we have a list L_{i-1} of states $|\psi_k\rangle$ satisfying $\mathrm{val}(k) \geq (i-1)\sqrt{m-1}$. From the list L_{i-1}, choose all distinct pairs $\{|\psi_k\rangle, |\psi_l\rangle\}$ such that $\mathrm{val}(k-l) \geq i\sqrt{m-1}$. For each such pair, use the above procedure to generate a state $|\psi_{k\pm l}\rangle$. Discard the result if the outcome is $k+l$, and create a new list L_i of all the resulting states of the form $|\psi_{k-l}\rangle$.

3. For the final list, relax the constraints to choose pairs so that $\mathrm{val}(k-l) = m-1$, and stop when such a state $|2^{m-1}\rangle$ is formed.

4. Measure the state $|\psi_{2^{m-1}}\rangle$ with respect to the $|\pm\rangle$ basis in order to determine the parity of ℓ.

All that remains is to argue that sufficiently many states were generated in (1) to guarantee conclusion in (4).

Note that at each stage, there are at most $2^{\lceil m-1\rceil}$ unmatched pairs, corresponding to the maximum possible distinct binary expansions of elements of L_{i-1} mod $2^{i\lceil\sqrt{m-1}\rceil}$. Moreover, for each pair the probability of measuring $k-l$ and proceeding to the next stage is $\frac{1}{2}$. Thus we know $|L_i| \geq \frac{1}{4}(|L_{i-1} - 2^{\lceil m-1\rceil})$, which gives inductively that

$$|L_i| \geq 2^{-2i}|L_0| - \sum_{j=1}^{i} 2^{\lceil m-1\rceil-2j} = 2^{-2i}|L_0| - \frac{1}{3}2^{\lceil m-1\rceil}(1-2^{-2i}).$$

Thus, to be sure that $|L_i| > 0$ when $i = \lceil m-1\rceil$, we must choose $|L_0| > \frac{1}{3}2^{3\lceil m-1\rceil}(1 - 2^{-2\lceil m-1\rceil}) = O(8^{\lceil m-1\rceil})$. Kuperberg makes this heuristic argument precise in [14].

Note that the beauty of Greg Kuperberg's idea is that it directly modifies (and tracks) the phase of one element in the superposition to obtain a desirable state. It bypasses the global phase, which is coset-dependent, entirely.

In the next section be propose a novel alternative approach that will instead capitalize on this global phase, by creating a unitary operator that will successfully extract a global phase (which carries some information about the coset), before obtaining more information through measurement.

4.4 Novel algorithms

4.4.1 DHSP and the Phase estimation algorithm

More often than not, the global phase carries a lot of interesting information that we would like to learn. Usually, in order to obtain some information about one of the basis states $|\phi\rangle$, we could simply perform a measurement with respect to the orthonormal basis. However, a simple measurement will not unveil anything about the global phase. So we must turn to another powerful tool, called the "phase estimation algorithm".

Let $\mathcal{H}$ be a Hilbert space. Suppose you have a state $|\phi\rangle \in \mathcal{H}$, and a unitary $U \in L(\mathcal{H})$ such that the resulting state after applying U to $|\phi\rangle$ is $\lambda|\phi\rangle$. That is, suppose $|\phi\rangle$ is one of the orthonormal basis eigenvectors of U such that $U|\phi\rangle = \lambda|\phi\rangle$, and the complex number λ is one of the eigenvalues of U of the form $\lambda = e^{2\pi i\theta}$. Then we can apply phase estimation algorithm to learn λ, given that the quantum controlled-U^{2^j} operations can be efficiently performed for any $j \in \{0, \ldots, t-1\}$.

If all of the above requirements are met, given U and $|\phi\rangle$, the phase estimation algorithm outputs both, the state $|\phi\rangle$, and a good approximation of θ. We sketch the idea of the algorithm as follows.

For simplicity, suppose that $\theta = a/2^t$ with $a \in \mathbb{Z}$ so that θ can be written in binary as $\theta = 0.\theta_1\theta_2\ldots\theta_t$. Then for $|b\rangle \in \{|0\rangle, |1\rangle\}$, recall that the controlled unitary c-$U^{2^j} \in L(\mathbb{C}^2 \otimes \mathcal{H})$, with control set at "1", sends $|b\rangle|\phi\rangle$ to

$$c\text{-}U^{2^j}|b\rangle|\phi\rangle = \begin{cases} |b\rangle(U^{2^j b})|\phi\rangle = e^{2\pi i 2^j \theta b}|b\rangle|\phi\rangle, & \text{if } b = 1, \\ |b\rangle|\phi\rangle, & \text{if } b = 0. \end{cases}$$

The phase estimation procedure requires two registers. The first register contains t qubits initialized to zero, and the second register contains the eigenstate $|\phi\rangle$. The procedure has t steps, indexed by $0 \le j \le t-1$. At step j, the procedure applies, to the $(j+1)$-th qubit of the first register, a Hadamard gate leading to a superposition of the form $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. This step is followed by a controlled unitary operator c-U^{2^j} that acts on the result and the second register via

$$c\text{-}U^{2^j}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\phi\rangle) = \frac{1}{\sqrt{2}}(c\text{-}U^{2^j}|0\rangle|\phi\rangle + c\text{-}U^{2^j}|1\rangle|\phi\rangle)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle|\phi\rangle + |1\rangle e^{2\pi i 2^j\theta}|\phi\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^j\theta}|1\rangle)|\phi\rangle$$

for all $j \in \{0, 1, \ldots, t-1\}$. Note that the state $|\phi\rangle$ remains unchanged even though we have been able to put θ into the phase of the first qubit.

The result after t steps is the state

$$\frac{1}{2^{\frac{t}{2}}}\bigotimes_{j=0}^{t-1}\Big(|0\rangle + e^{2\pi i 2^j\theta}|1\rangle\Big)\otimes|\phi\rangle.$$

Note that if $(0.\theta_0\theta_1\ldots\theta_{t-1}) = \theta_0 2^{-1}+\theta_1 2^{-2}+...+\theta_{t-1}2^{-t}$ is a binary fraction of θ, then $\frac{1}{\sqrt{2^t}}\bigotimes_{j=0}^{t-1}(|0\rangle+e^{2\pi i 2^j\theta}|1\rangle)$ is actually equivalent to $F_{2^t}|\theta\rangle$, where F_{2^t} is a QFT [19, Section 5.1, equation 5.4]. Therefore, we can rewrite $\frac{1}{2^{\frac{t}{2}}}\bigotimes_{j=0}^{t-1}\Big(|0\rangle + e^{2\pi i 2^j\theta}|1\rangle\Big)\otimes|\phi\rangle$ as $F_{2^t}|\theta\rangle\otimes|\phi\rangle$.

After applying the inverse QFT to the first register, the resulting state is

$$F_{2^t}^{-1}\otimes I(F_{2^t}|\theta\rangle\otimes|\phi\rangle) = F_{2^t}^{-1}F_{2^t}|\theta\rangle\otimes I|\phi\rangle = |\theta\rangle\otimes|\phi\rangle.$$

So the state in the first register is $|\theta\rangle$, and $|\phi\rangle$ remains intact in the second register. From here we can read θ by measuring the first register in the computational basis.

The algorithm in [14] also focuses on the phase, rather than the state. However Greg Kuperberg is interested in the phase that carries data about the hidden reflection, and not the global phase. A natural question would be whether or not we can use the global phase instead?

Let $G = D_{2n}$. We will view G as $\mathbb{Z}/n\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$. Let $\mathcal{H}$ be a Hilbert space spanned by the elements of $\mathbb{Z}/n\mathbb{Z}$. Let U' be the unitary on $\mathcal{H}$ that for each $g\in\mathbb{Z}/n\mathbb{Z}$ acts on $|g\rangle$ as

$$U'|g\rangle = e^{\frac{2\pi i g}{n}}|g\rangle.$$

Then the unitary $U = U'\otimes I$ on $\mathcal{H}\otimes\mathbb{C}^2$ acts on $|g\rangle\otimes|b\rangle$ as

$$U(|g\rangle\otimes|b\rangle) = e^{\frac{2\pi i g}{n}}|g\rangle\otimes|b\rangle.$$

Let $H = \langle r^k s\rangle$ be the hidden subgroup. Suppose that we start with a coset state of the form $|r^aH\rangle = \frac{1}{\sqrt{2}}(|a\rangle|0\rangle + |a+k\rangle|1\rangle)$. Then after applying the unitary U, the resulting state is

$$\begin{aligned}U|r^aH\rangle &= \frac{1}{\sqrt{2}}(e^{\frac{2\pi i a}{n}}|a\rangle|0\rangle + e^{\frac{2\pi i(a+k)}{n}}|a+k\rangle|1\rangle)\\ &= \frac{1}{\sqrt{2}}e^{\frac{2\pi i a}{n}}(|a\rangle|0\rangle + e^{\frac{2\pi i l}{n}}|a+k\rangle|1\rangle).\end{aligned}$$

The global phase has some information about a coset representative.

Suppose that we could apply the phase estimation algorithm to the state $|r^aH\rangle$ in order to obtain some information about the coset representative a. Suppose that then we measure the first qubit of the state $|r^aH\rangle$ with respect to the basis of $\mathcal{H}$, this will yield the state $|a+k\rangle$ with probability $p=\frac{1}{2}$. Given that we are lucky and were able to obtain $a+k$ from the measurement, it will be possible to deduce something about the hidden reflection k. Unfortunately, we cannot use the phase estimation algorithm in this case, the reason being $U\frac{1}{\sqrt{2}}(|a\rangle|0\rangle + |a+k\rangle|1\rangle) \neq \frac{1}{\sqrt{2}}e^{\frac{2\pi ia}{n}}(|a\rangle|0\rangle + |a+k\rangle|1\rangle)$.

We were working to see whether a similar idea would lead to an efficient algorithm, and we will show that unfortunately the idea we have outlined below does not solve the Dihedral HSP.

Suppose $G = D_{2n}$, and hidden subgroup $H = \langle r^k s\rangle$ is generated by a hidden reflection. Here we will again view G as a semi-direct product $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Let $\mathcal{H}$ be a Hilbert space spanned by the elements of $\mathbb{Z}/n\mathbb{Z}$. Using the standard method we can create a coset state

$$|cH\rangle = \frac{1}{\sqrt{2}}(|c\rangle|0\rangle + |c+k\rangle|1\rangle).$$

Define a unitary U'' acting on $\mathcal{H} \otimes \mathbb{C}^2$ via

$$U''(|a\rangle \otimes |b\rangle) = \begin{cases} |a\rangle \otimes |b\rangle, & \text{if } a \text{ is even;} \\ -|a\rangle \otimes |b\rangle, & \text{else.} \end{cases}$$

Notice that if k is even, then if we apply the unitary operator U'' to the coset state, we will get $U''|cH\rangle = \pm\frac{1}{\sqrt{2}}(|c\rangle|0\rangle + |c+k\rangle|1\rangle)$, regardless of the of c. We can rewrite it as

$$U''|cH\rangle = \begin{cases} |cH\rangle, \text{if } c \text{ is even;} \\ -|cH\rangle, \text{if } c \text{ is odd.} \end{cases}$$

Thus, when k is even, the coset state $|cH\rangle$ is an eigenvector of the unitary transformation U'' with eigenvalues $e^{\pi i}$ and $e^{2\pi i}$. This gives us freedom, to apply the phase estimation procedure successfully to conclude the parity of c. After the phase estimation procedure, the state in the second register is $\frac{1}{\sqrt{2}}(|c\rangle|0\rangle + |c+k\rangle|1\rangle)$. So we could gain some additional information by measuring the first qubit with respect to the orthonormal basis of $\mathcal{H}$.

On the other hand, if k is odd, then the signs will be different for two elements of the superposition, yielding $U''|cH\rangle = \frac{1}{\sqrt{2}}(|c\rangle|0\rangle - |c+k\rangle|1\rangle)$ or $\frac{1}{\sqrt{2}}(-|c\rangle|0\rangle + |c+k\rangle|1\rangle)$. Which we can rewrite as

$$U''|cH\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|c\rangle|0\rangle - |c+k\rangle|1\rangle), \text{if } c \text{ if even;} \\ -\frac{1}{\sqrt{2}}(|c\rangle|0\rangle - |c+k\rangle|1\rangle), \text{if } c \text{ is odd.} \end{cases}$$

Since the coset state is not an eigenvector of U'', if we apply the phase estimation procedure it will fail in the general sense i.e. it will not produce an approximation of the phase. Unfortunately, this means that when k is odd we won't be able to determine the parity of c using this approach.

4.4.2 Collapsing a perfect superposition to a known chosen state

Let $\mathcal{H}$ be a Hilbert spaced spanned by the set of orthonormal vectors $B = \{|\psi_j\rangle \mid 0 \leq j < 2^n\}$. Suppose that we have a uniform superposition of the basis states

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |\psi_j\rangle,$$

and we would like to transform $|\psi\rangle$ to a given known state $|\psi_{target}\rangle \in B$. We cannot do so using measurement with certainty, instead, if we use projective measurement operators with respect to the basis B we will obtain $|\psi_{target}\rangle$ with probability $p = \frac{1}{2^n}$. Ahmed Younes and Mahmoud Abdel-Aty in [25] proposed an efficient quantum algorithm for transforming the superposition $|\psi\rangle$ to a chosen state $|\psi_{target}\rangle$; they called this collapsing without a measurement. Before we state the algorithms we will introduce some results that we will use repeatedly later in this section. Suppose that the binary representation of ψ_j is $j_0 \ldots j_{n-1}$ for any $j \in \{0, \ldots, 2^n - 1\}$, so in $\mathcal{H}$ we have $|\psi_j\rangle = |j_0\rangle|j_1\rangle \cdots |j_{n-1}\rangle$.

Lemma 4.4.1. *Let X and Y be the Pauli gates and let $|\psi_{target}\rangle \in \mathcal{H}$ be our target vector. Define $U_1 \in \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^2)$ by*

$$U_1 = \sum_{j=0, j\neq target}^{2^{n-1}} |\psi_j\rangle\langle\psi_j| \otimes XY + |\psi_{target}\rangle\langle\psi_{target}| \otimes I. \tag{4.4.1}$$

Then U_1 is unitary.

Proof: Recall that

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

so

$$XY = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

Let us confirm that U_1 is unitary. Let

$$U_1{}^* = \sum_{j=0, j\neq target}^{2^n-1} |\psi_j\rangle\langle\psi_j| \otimes Y^*X^* + |\psi_{target}\rangle\langle\psi_{target}| \otimes I$$

be a linear operator. Since $\sum_{j=0}^{2^n-1} |\psi_j\rangle\langle\psi_j| = I$, it can be easily shown that the product U^*U is

$$(\sum_{j=0, j\neq target}^{2^n-1} |\psi_j\rangle\langle\psi_j| \otimes Y^*X^* + |\psi_{target}\rangle\langle\psi_{target}| \otimes I)(\sum_{j=0, j\neq target}^{2^n-1} |\psi_j\rangle\langle\psi_j| \otimes XY + |\psi_{target}\rangle\langle\psi_{target}| \otimes I)$$

$$\begin{aligned}
&= \sum_{j=0, j\neq target}^{2^n-1} |\psi_j\rangle\langle\psi_j| \otimes Y^*X^*XY + |\psi_{target}\rangle\langle\psi_{target}| \otimes I \\
&= \sum_{j=0, j\neq target}^{2^n-1} |\psi_j\rangle\langle\psi_j| \otimes I + |\psi_{target}\rangle\langle\psi_{target}| \otimes I \\
&= \sum_{j=0}^{2^n-1} |\psi_j\rangle\langle\psi_j| \otimes I \\
&= I.
\end{aligned}$$

$\blacksquare$

Now define the Hamming distance $D(\psi_x, \psi_y)$ between ψ_x and ψ_y as the number of 1s in the binary expansion of $\psi_x \oplus \psi_y$. That is, if we expand

$$|\psi_x\rangle = |x_0\rangle|x_1\rangle \cdots |x_{n-1}\rangle \in (\mathbb{C}^2)^{\otimes n}$$

and similarly for $|\psi_y\rangle$, then

$$D(\psi_x, \psi_y) = \sum_{i=0}^{n-1} x_i \oplus y_i.$$

So the Hamming distance uses the indices of the states. Thus, we can define the following function. Given an index of the target state $target \in \{0, 1, \ldots, 2^n - 1\}$, define a function $s\colon \{0, 1, \ldots, 2^n - 1\} \to \mathbb{Z}/4\mathbb{Z}$ by

$$s(j) = \begin{cases} 0 & \text{if } j = target \\ D(\psi_{target}, \psi_j) - 1 & \text{if } j \neq target. \end{cases}$$

Lemma 4.4.2. *Define $U_2 \in \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^2)$ by*

$$U_2 = \sum_{j=0}^{2^n-1} e^{\frac{\pi i s(j)}{2}} |\psi_j\rangle\langle\psi_j| \otimes I. \tag{4.4.2}$$

Then U_2 is unitary.

Proof: With respect to the standard basis, U_2 is a diagonal matrix with elements of norm 1 on the diagonal, so it is unitary. ▮

Now let $U_3 \in \mathcal{L}(\mathbb{C}^2)$ be defined with respect to the standard basis by

$$U_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}.$$

This is a unitary matrix and it has the property that

$$U_3^2 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

In particular, we can write this as saying

$$U_3^2|x\rangle = i|\overline{x}\rangle = e^{\frac{\pi i}{2}}|\overline{x}\rangle$$

where $\overline{0} = 1$ and $\overline{1} = 0$.

Lemma 4.4.3. *For $x \in \{0, 1\}$, we have*

$$U_3|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0,1} e^{\frac{\pi i \overline{x} \oplus z}{2}} |z\rangle.$$

Proof: Note that $\overline{x} \oplus z$ is equal to either 1 or 0, depending on whether they are equal or not, respectively. When it is 0 we have $e^{\frac{\pi i \overline{x} \oplus z}{2}} = 1$, and when it is 1 we have $e^{\frac{\pi i \overline{x} \oplus z}{2}} = i$. So this expression describes the matrix U_3. ▮

Applying this transformation U_3 to each of the qubits comprising $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ gives us our final transformation.

Lemma 4.4.4. *Let $|\psi_y\rangle = |y_0\rangle|y_1\rangle \cdots |y_{n-1}\rangle \in \mathcal{H}$. Then*

$$U_3^{\otimes n}|\psi_y\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{\frac{\pi i D(\overline{\psi_y}, \psi_z))}{2}} |\psi_z\rangle. \tag{4.4.3}$$

Proof:

$$
\begin{aligned}
U_3^{\otimes n}|\psi_y\rangle &= U_3^{\otimes n}|y_0\rangle|y_1\rangle\ldots|y_{n-1}\rangle \\
&= |U_3|y_0\rangle\rangle|U_3|y_1\rangle\rangle\ldots|U_3|y_{n-1}\rangle\rangle \\
&= |\sum_{z_0=0,1} e^{\frac{\pi i(\overline{y_0}\oplus z_0)}{2}}|z_1\rangle\rangle|\sum_{z_1=0,1} e^{\frac{\pi i(\overline{y_1}\oplus z_1)}{2}}|z_1\rangle\rangle\cdots|\sum_{z_{n-1}=0,1} e^{\frac{\pi i(\overline{y_{n-1}}\oplus z_{n-1})}{2}}|z_{n-1}\rangle\rangle \\
&= \sum_{z_0=0,1;z_1=0,1;\ldots z_{n-1}=0,1} |e^{\frac{\pi i(\overline{y_0}\oplus z_0)}{2}}|z_0\rangle\rangle|e^{\frac{\pi i(\overline{y_1}\oplus z_1)}{2}}|z_1\rangle\rangle\cdots|e^{\frac{\pi i(\overline{y_{n-1}}\oplus z_{n-1})}{2}}|z_{n-1}\rangle\rangle \\
&= \sum_{z=0}^{2^n-1}\prod_{j=0}^{n-1} e^{\frac{\pi i(\overline{y_j}\oplus z_j)}{2}}|z_0\rangle|z_1\rangle\cdots|z_{n-1}\rangle \\
&= \sum_{z=0}^{2^{n-1}} e^{\frac{\pi i}{2}\sum_{j=0}^{n-1}\overline{y_j}\oplus z_j}|z_0\rangle|z_1\rangle\cdots|z_{n-1}\rangle \\
&= \sum_{z=0}^{2^n-1} e^{\frac{\pi i}{2}\overline{\psi_y}\oplus\psi_z}|\psi_z\rangle \\
&= \sum_{z=0}^{2^n-1} e^{\frac{\pi i}{2}D(\overline{\psi_y},\psi_z})|\psi_z\rangle.
\end{aligned}
$$

∎

From the fact that $U_3^2|x\rangle = i|\overline{x}\rangle$ for some $|x\rangle \in \{|0\rangle, |1\rangle\}$ we can deduce the following lemma.

Lemma 4.4.5. *For any $|\psi_y\rangle = |y_0\rangle|y_1\rangle\cdots|y_{n-1}\rangle \in \mathcal{H}$, we have*

$$U_3^{\otimes n}U_3^{\otimes n}|\psi_y\rangle = i^n|\overline{\psi_y}\rangle$$

where $|\overline{\psi_y}\rangle = |\overline{y_0}\rangle|\overline{y_1}\rangle\cdots|\overline{y_{n-1}}\rangle$.

Proof:

$$
\begin{aligned}
U_3^{\otimes n}U_3^{\otimes n}|\psi_y\rangle &= U_3^{\otimes n}U_3^{\otimes n}|y_0\rangle|y_1\rangle\ldots|y_{n-1}\rangle \\
&= U_3U_3|y_0\rangle U_3U_3|y_1\rangle\ldots U_3U_3|y_{n-1}\rangle \\
&= i|\overline{y_0}\rangle i|\overline{y_1}\rangle\cdots i|\overline{y_{n-1}}\rangle \\
&= i^n|\overline{y_0}\rangle|\overline{y_1}\rangle\cdots|\overline{y_{n-1}}\rangle \\
&= i^n|\overline{\psi_y}\rangle
\end{aligned}
$$

Thus,

$$U_3^{\otimes n}U_3^{\otimes n}|\psi_y\rangle = i^n|\overline{\psi_y}\rangle \tag{4.4.4}$$

■

The algorithm in [25] goes as follows.

Step 1: Given the input state $|\psi\rangle \otimes |0\rangle$, apply unitary U_1 as defined in the Lemma 4.4.1. The resulting state is $|\psi_1\rangle$ given by

$$U_1|\psi\rangle \otimes |0\rangle = i(\frac{1}{\sqrt{2^n}} \sum_{j=0, j\neq target}^{2^n-1} |\psi^j\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2^n}}|\psi_{target}\rangle \otimes |0\rangle. \tag{4.4.5}$$

Step 2: Apply unitary U_2 as defined in the Lemma 4.4.2 to the new state $|\psi_1\rangle$. The resulting state is $|\psi_2\rangle$ given by

$$\begin{aligned} U_2|\psi_1\rangle &= (i\frac{1}{\sqrt{2^n}} \sum_{j=0, j\neq target}^{2^n-1} e^{\frac{\pi i s(j)}{2}} |\psi_j\rangle \otimes |0\rangle) + e^{\frac{\pi i s(target)}{2}} \frac{1}{\sqrt{2^n}}|\psi_{target}\rangle \otimes |0\rangle \\ &= i\frac{1}{\sqrt{2^n}}(\sum_{j=0, j\neq k}^{2^n-1} e^{\frac{\pi i D(\psi_j,\psi_{target})-1}{2}} |\psi_j\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2^n}} e^{\frac{\pi i D(\psi_{target},\psi_{target})}{2}} |\psi_{target}\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2^n}}(\sum_{j=0, j\neq k}^{2^n-1} e^{\frac{\pi i D(\psi_j,\psi_{target})}{2}} |\psi_j\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2^n}} e^{\frac{\pi i D(\psi_{target},\psi_{target})}{2}} |\psi_{target}\rangle \otimes |0\rangle \end{aligned}$$

since $ie^{\frac{\pi i D(\psi_j,\psi_{target})-1}{2}} = e^{\frac{\pi i}{2}} e^{\frac{\pi i D(\psi_j,\psi_{target})-1}{2}} = e^{\frac{\pi i D(\psi_j,\psi_{target})}{2}}$. That is, we have

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{\frac{\pi i D(\psi_j,\psi_{target})}{2}} |\psi_j\rangle \otimes |0\rangle.$$

Note that we can rewrite $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{\frac{\pi i D(\psi_j,\psi_{target})}{2}} |\psi_j\rangle \otimes |0\rangle$ as

$$\frac{1}{\sqrt{2^n}} {U_3}^{\otimes n} |\overline{\psi}_{target}\rangle \otimes |0\rangle$$

by Lemma 4.4.4.

Step 3: Apply unitary $U_3^{\otimes n} \otimes I$, where $U_3^{\otimes n}$ is as defined in the Lemma 4.4.4 to the state $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} {U_3}^{\otimes n} |\overline{\psi}_{target}\rangle \otimes |0\rangle$. By Lemma 4.4.5, the resulting state is

$$e^{\frac{\pi i n}{2}} |\psi_{target}\rangle \otimes |0\rangle = i^n |\psi_{target}\rangle \otimes |0\rangle.$$

The reader might have noticed right away that the algorithm as it is, is not very interesting since $|\psi_{target}\rangle$ being one of the orthonormal basis vectors can be easily produces and simply stored in another register. What we focused our attention instead is whether we will be able to transform a perfect superposition of states to a partially-known state. As our input states, we will consider states of the form $\frac{1}{\sqrt{|H|}}\sum_{h\in H}|ch\rangle\otimes|f(c)\rangle$, where H is the hidden subgroup and f is the hiding function. Now our target state will be of the form $\frac{1}{\sqrt{|H|}}\sum_{h\in H}|h\rangle\otimes|f(e)\rangle$, where $|f(e)\rangle$ is known from evaluating the function f on the identity elements of G. Let us try to use the above algorithm to see if we can find H for $G = D_{2N}$.

Let $G = D_{2N}$ where $N = 2^n$. Let H be a hidden subgroup generated by the reflection $r^k s$. Let $X = \{0, \cdots, N-1\}$ and suppose $f\colon G \to X$ is the hiding function. Since we want to find a reflection only, and since each reflection is in a distinct coset of H, it suffices to work on reflections only.

Query $f(e)$ and call the answer x_k. Our goal is to find $r^k s$. Our target state is $|\psi_{ideal}\rangle = |r^k s\rangle \otimes e^{\frac{\pi i n}{2}}|x_k\rangle \otimes |0\rangle$. Our notation will be that $f(r^j s) = x_j \in X$. Note that we do not know $r^k s$, but we do know $f(e) = x_k$, and the two states are entangled. So it is reasonable to expect that replicating the above algorithm with some information about one state might help us learn enough information about both.

Let $\mathcal{H}_1$ be a Hilbert space spanned by the reflections of D_{2n}. Let $\mathcal{H}_2$ be a Hilbert space spanned by the elements of the set X. The algorithm goes as follows.

Prepare three registers. Prepare the first register is a uniform superposition of all the reflections of D_{2n}, the second storing states of $\mathcal{H}_2$, initially set to $|0\rangle$. Prepare the last register storing states of $\mathbb{C}^2$, initialized to $|0\rangle$.

Step 1: Perform steps 1-2 of the standard method on the first two registers to arrive at the state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|r^j s\rangle \otimes |x_j\rangle \otimes |0\rangle.$$

Step 2: Apply the unitary $U_1' = I \otimes U_1$ to the state $|\psi\rangle$, where U_1 is as in Lemma 4.4.1 with target $|x_k\rangle$. The resulting state is

$$U_1'|\psi\rangle = |\psi_1\rangle = i\left(\frac{1}{\sqrt{2^n}}\sum_{j=0,j\neq k}^{2^n-1}|r^j s\rangle \otimes |x_j\rangle \otimes |0\rangle\right) + \frac{1}{\sqrt{2^n}}|r^k s\rangle\otimes|x_k\rangle\otimes|0\rangle. \quad (4.4.6)$$

Step 3: Apply the unitary $U_2' = I \otimes U_2$, where U_2 is as in Lemma 4.4.2, to the state $|\psi_1\rangle$. The resulting state $|\psi_2\rangle$ is

$$\begin{aligned}
U_2'|\psi_1\rangle &= i(\frac{1}{\sqrt{2^n}} \sum_{j=0, j\neq k}^{2^n-1} e^{\frac{\pi i s(j)}{2}} |r^j s\rangle \otimes |x_j\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2^n}} e^{\frac{\pi i s(k)}{2}} |r^k s\rangle \otimes |x_k\rangle \otimes |0\rangle \\
&= i(\frac{1}{\sqrt{2^n}} \sum_{j=0, j\neq k}^{2^n-1} e^{\frac{\pi i D(x_j,x_k)-1}{2}} |r^j s\rangle \otimes |x_j\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2^n}} e^{\frac{\pi i D(x_k,x_k)}{2}} |r^k s\rangle \otimes |x_k\rangle \otimes |0\rangle \\
&= (\frac{1}{\sqrt{2^n}} \sum_{j=0, j\neq k}^{2^n-1} e^{\frac{\pi i D(x_j,x_k)}{2}} |r^j s\rangle \otimes |x_j\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2^n}} e^{\frac{\pi i D(x_k,x_k)}{2}} |r^k s\rangle \otimes |x_k\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{\frac{\pi i D(x_j,x_k)}{2}} |r^j s\rangle \otimes |x_j\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |r^j s\rangle \otimes e^{\frac{\pi i D(x_j,x_k)}{2}} |x_j\rangle \otimes |0\rangle
\end{aligned}$$

Step 4: Apply the unitary $U_3' = I \otimes {U_3}^{\otimes n} \otimes I$, where ${U_3}^{\otimes n}$ is defined as in Lemma 4.4.4 to the state $|\psi_2\rangle$. The resulting state is

$$\begin{aligned}
U_3'|\psi_2\rangle &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |r^j s\rangle \otimes e^{\frac{\pi i D(x_j,x_k)}{2}} {U_3}^{\otimes n} |x_j\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |r^j s\rangle \otimes e^{\frac{\pi i D(x_j,x_k)}{2}} (\sum_{l=0}^{2^n-1} e^{\frac{\pi i D(\overline{x}_j,x_l)}{2}} |x_l\rangle) \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |r^j s\rangle \otimes \sum_{l=0}^{2^n-1} e^{\frac{\pi i}{2} D(\overline{x}_j,x_l)+D(x_j,x_k)} |x_l\rangle \otimes |0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{l=0}^{2^n-1} |r^j s\rangle \otimes e^{\frac{\pi i}{2} D(\overline{x}_j,x_l)+D(x_j,x_k)} |x_l\rangle \otimes |0\rangle.
\end{aligned}$$

Notice that the result we are looking for is $|\psi_{ideal}\rangle = |r^k s\rangle \otimes e^{\frac{\pi i n}{2}} |x_k\rangle \otimes |0\rangle$, since measuring the first register in the standard basis would lead the hidden reflection and consequently the hidden subgroup. Unfortunately, the resulting state $U_3'|\psi_2\rangle$ is equal to $|\psi_{ideal}\rangle$ if and only if $D(x_j, x_k) + D(\overline{x}_j, x_l) = 0 \pmod 4$. Since this is not always true, we conclude that performing Steps 1–3 of this algorithm does not transform the input state into our chosen target partially-known state. So unfortunately, this approach did not directly yield a solution to the HSP.

4.4.3 Additional results

While entertaining ourselves with the different variations of the algorithm in the previous section, we produced a peculiar example below. Note that in this example we do not apply the algorithm exactly as in the previous section, but rather use the unitary operators, as defined in the Lemma 4.4.1, Lemma 4.4.2, and Lemma 4.4.4 in a new way.

Example. Let $G = D_8$. Let $H = \langle r^2 s\rangle$. Let the elements of G be represented by binary numbers as

$$e = 000, r = 001, r^2 = 010, r^3 = 100$$
$$s = 011, rs = 101, r^2 s = 110, r^3 s = 111.$$

Suppose that after applying Steps 1–3 of the standard method we have the following coset state

$$|rH\rangle = \frac{1}{\sqrt{2}}(|r\rangle + |r^3 s\rangle).$$

For every element $g \in G$, consider the following linear operator

$$U_1 = \sum_{g\in G} e^{\frac{\pi i D(g,e)}{2}} |g\rangle\langle g|,$$

where $D(g, e)$ is the Hamming distance between binary strings associated to g and e. This operator is a unitary since it is a diagonal matrix with unit elements along the diagonal. The unitary U_1 was inspired by the unitary operators in the Lemma 4.4.1, and Lemma 4.4.2.

Apply U_1 to the coset state $|rH\rangle = \frac{1}{\sqrt{2}}(|r\rangle + |r^3 s\rangle)$. The resulting state is

$$\begin{aligned}|\psi\rangle &= U_1|rH\rangle \\ &= \frac{1}{\sqrt{2}}(U_1|r\rangle + U_1|r^3 s\rangle) \\ &= \frac{1}{\sqrt{2}}(e^{\frac{\pi i D(r,e)}{2}}|r\rangle + e^{\frac{\pi i D(r^3 s,e)}{2}}|r^3 s\rangle) \\ &= \frac{1}{\sqrt{2}}(i|r\rangle + -i|r^3 s\rangle).\end{aligned}$$

Now apply ${U_3}^{\otimes 3}$ twice as defined in the Lemma 4.4.5 to the state $|\psi\rangle$. Then the resulting state $|\phi\rangle$ is

$$\begin{aligned}{U_3}^{\otimes 3}{U_3}^{\otimes 3}|\psi\rangle &= \frac{1}{\sqrt{2}}(i{U_3}^{\otimes 3}{U_3}^{\otimes 3}|r\rangle + -i{U_3}^{\otimes 3}{U_3}^{\otimes 3}|r^3 s\rangle) \\ &= \frac{1}{\sqrt{2}}(i(i^3)|\overline{r}\rangle - i(i^3)|\overline{r^3 s}\rangle) \\ &= \frac{1}{\sqrt{2}}(|r^2 s\rangle - |e\rangle).\end{aligned}$$

Now measuring the state $\frac{1}{\sqrt{2}}(|r^2s\rangle - |e\rangle)$ with respect to the standard basis yields the hidden reflection r^2s with probability $p = \frac{1}{2}$.

Suppose that the coset state is $\frac{1}{\sqrt{2}}(|r^i\rangle + |r^{i+2}s\rangle)$ for some $0 \leq i < n$. Then after applying the unitary U_1, and unitary ${U_3}^{\otimes 3}$ twice we get

$$\frac{1}{\sqrt{2}}(e^{\frac{\pi i}{2}D(r^i,e)+3}|\overline{r^i}\rangle + e^{\frac{\pi i}{2}D(r^{i+2}s,e)+3}|\overline{r^{i+2}s}\rangle).$$

In the example above, a clever way of assigning the binary representation to the elements of G guaranteed that the final state $\frac{1}{\sqrt{2}}(|r^2s\rangle - |e\rangle)$ is precisely constructed from the elements of H. In the general case, we would require that $\overline{r^i}$, and $\overline{r^{i+2}s}$ are both elements of H.

So we assume that there is more structure to this approach that we need to investigate further. We would like to know whether different choices of binary representations for the elements of G, or applying some clever unitary operators would leak some information about the hidden subgroup from these ideas. So if the adversary know something about the Hamming distance between the elements, perhaps it would be possible to design a more sophisticated and efficient attack.

4.4.4 Coset tensors algorithm

The following quantum algorithm is drastically different from any quantum algorithms that we have considered so far. The idea of this algorithm is to step back from the standard method and reconsider coset states. One of the apparent challenges of the standard method, is that given a coset state we could only ever get a single element of the coset after the measurement, and we could not easily reproduce the same coset state again. This algorithm challenges the idea of the coset state being of the form $|cH\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|ch\rangle$. Instead, we consider cosets of the form $|cH\rangle = \bigotimes_{h\in H}|ch\rangle$.

Let $G = D_{2n}$. Let X be a finite set. Suppose $H = \langle r^l s\rangle$ is a hidden subgroup generated by a reflection, and $f : G \mapsto X$ is a function hiding H. Let $\mathcal{H}_1$ be a Hilbert space generated by all the rotations in G, and let $\mathcal{H}_2$ be a Hilbert space generated by all the reflections in G. The algorithm goes as follows.

Step 1: Prepare $n + 2$ registers. Let the first register store elements of $\mathcal{H}_1$. Prepare the first register in a uniform superposition of all rotations of G, namely $\frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|r^i\rangle$. Let the second register store elements of $\mathcal{H}_2$. Prepare the second register in a uniform superposition of all the reflections of G, namely $\frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}|r^j s\rangle$. Let the last n registers store the data from $\mathbb{C}^2$, all initialized to zero. So the initial state is

$$\begin{aligned}|\phi_1\rangle &= \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|r^i\rangle \otimes \frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}|r^j s\rangle \otimes |0\rangle^{\otimes n} \\ &= \frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}|r^i\rangle \otimes |r^j s\rangle \otimes |0\rangle^{\otimes n} = |\psi_1\rangle \otimes |0\rangle^{\otimes n}\end{aligned}$$

Suppose that S is a set of all subgroups of G generated by a reflection element in G. Let S' be a set of all possible cosets of all the subgroups in S. Then the state $|\psi_1\rangle$ is a uniform superposition of tensor products of the coset elements of all the cosets in S'. There are n^2 such tensor products, and only n of them are tensor products of the coset elements of the cosets of H. We would like to have a way of distinguishing between "good" cosets i.e. tensor products of the coset elements of H, and "bad" cosets of other subgroups. Note that for any $g_1 \in \mathcal{H}_1, g_2 \in \mathcal{H}_2$, the coset $|g_1\rangle \otimes |g_2\rangle$ is good if and only if $f(g_1) = f(g_2)$. Equivalently, we can say that the good coset is of the form $|r^i\rangle \otimes |r^{i+l}s\rangle$, for some $0 \leq i < n$. So we would like to create a unitary operator that compares functional values of the elements in the first, and the second register, and then "mark" the good states so we can set them apart from the bad ones.

For each i, we will define a unitary that compares $f(g_1)$, for some $g_1 \in \mathcal{H}_1$, and $f(g_2)$, for some $g_2 \in \mathcal{H}_2$, and then depending on the result of the comparison flips the state in the i-th register among the last n registers. Suppose that $X_i \in L((\mathbb{C}^2)^{\otimes n})$ is the i-th bit flip operator. Let $|a\rangle = |a_1\rangle|a_2\rangle \dots |a_n\rangle \in (\mathbb{C}^2)^{\otimes n}$. Then the action of X_i on $|a\rangle$ is

$$X_i|a\rangle = \begin{cases} |a_1\rangle \dots \underbrace{|1\rangle}_{|a_i\rangle} \dots |a_n\rangle, & \text{if } a_i = 0; \\ |a_1\rangle \dots \underbrace{|0\rangle}_{|a_i\rangle} \dots |a_n\rangle, & \text{if } a_i = 1. \end{cases}$$

Define a linear operator $U_i \in L(\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes (\mathbb{C}^2)^{\otimes n})$ acting on the state $|g_1\rangle \otimes |g_2\rangle \otimes |a\rangle$ as

$$U_i(|g_1\rangle \otimes |g_2\rangle \otimes |a\rangle) = \begin{cases} |g_1\rangle \otimes |g_2\rangle \otimes X_i|a\rangle, & \text{if } f(g_1) = f(g_2); \\ |g_1\rangle \otimes |g_2\rangle \otimes |a\rangle, & \text{if } f(g_1) \neq f(g_2). \end{cases}$$

So U_i examines whether the coset is good, and if it is, it flips the bit in the i-th register among the last n registers.

Recall we initialized the last n registers to 0. Since there are only n good cosets, and n^2 bad cosets, it would not be efficient to measure the last n registers, hoping to obtain the result that has at least one "1". One way to conquer this problem is to create more good cosets. Note that the cosets of the subgroup $K = \langle r^{l+1}s\rangle$ look like $|r^i\rangle \otimes |r^{i+(l+1)}s\rangle$. Suppose that we can change the first state of the tensor product from $|r^i\rangle$ to $|r^{i+1}\rangle$. Then the "bad" coset $|r^i\rangle \otimes |r^{i+(l+1)}s\rangle$ of K is transformed into the "good" coset $|r^{i+1}\rangle \otimes |r^{(i+1)+l}s\rangle$, that is, a coset of H. So we should define a unitary that will alter the state in the first register for the bad cosets.

Recall that $|a\rangle = |a_1\rangle|a_2\rangle \dots |a_n\rangle \in (\mathbb{C}^2)^{\otimes n}$. Define a conditional unitary operator U_{r_i} acting on $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes (\mathbb{C}^2)^{\otimes n}$ via

$$U_{r_i}(|g_1\rangle \otimes |g_2\rangle \otimes |a\rangle) = \begin{cases} |g_1\rangle \otimes |g_2\rangle \otimes |a\rangle, & \text{if } a_i = 1, \\ |rg_1\rangle \otimes |g_2\rangle \otimes |a\rangle, & \text{if } a_i = 0. \end{cases}$$

Note that U_{r_i} only alters tensors of coset states that are not cosets of H by inspecting the i-th state of the last n states.

So the remaining steps of the algorithm simply perform "cycles" that consist of creating good cosets, by altering the state in the first register of the bad cosets, and then marking new good cosets. We will do the first few cycles in detail in Steps 2–4. Notice, however, that the state produced in Step 1 already has some good cosets, so the first cycle is Step 1–2, and the second cycle is Step 3–4.

Step 2: Apply the linear operator U_1 acting on $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes (\mathbb{C}^2)^{\otimes n}$ to the state $|\phi_1\rangle$. The resulting state is

$$|\phi_2\rangle = \frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0, j\neq i+l}^{n-1} |r^i\rangle \otimes |r^j s\rangle \otimes |0\rangle^{\otimes n} + \frac{1}{n}\sum_{i=0}^{n-1} |r^i s\rangle \otimes |r^{i+l}s\rangle \otimes |1\rangle \otimes |0\rangle^{\otimes(n-1)}$$

Notice how the unitary U_1 separated the good and the bad cosets, and changed the state in the first register among the last n registers for the good cosets only.

Step 3: Apply the unitary operator U_{r_1} to the state $|\phi_2\rangle$. The resulting state is

$$|\phi_3\rangle = \frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0, j\neq i+l}^{n-1} |r^{i+1}\rangle \otimes |r^j s\rangle \otimes |0\rangle^{\otimes n} + \frac{1}{n}\sum_{i=0}^{n-1} |r^i\rangle \otimes |r^{i+l}s\rangle \otimes |1\rangle \otimes |0\rangle^{\otimes(n-1)}$$

$$= \frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0, j\neq i+l, j\neq i+1+l}^{n-1} |r^{i+1}\rangle \otimes |r^j s\rangle \otimes |0\rangle^{\otimes n} + \frac{1}{n}\sum_{i=0}^{n-1} |r^i\rangle \otimes |r^{i+l}s\rangle \otimes |1\rangle \otimes |0\rangle^{\otimes(n-1)}$$

$$+\frac{1}{n}\sum_{i=0}^{n-1} |r^{i+1}\rangle \otimes |r^{(i+1)+l}s\rangle \otimes |0\rangle^{\otimes n}$$

Now, there are $2n$ good cosets. However, only n of them are marked.

Step 4: Apply a linear operator U_2 acting on $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes (\mathbb{C}^2)^{\otimes n}$ to the state $|\phi_2\rangle$. The resulting state is

$$|\phi_3\rangle = \frac{1}{n}\sum_{i=0}\sum_{j=0,j\neq i+l,j\neq i+1+l}^{n-1} |r^{i+1}\rangle\otimes|r^j s\rangle\otimes|0\rangle^{\otimes n}+\frac{1}{n}\sum_{i=0}^{n-1}|r^i\rangle\otimes|r^{i+l}s\rangle\otimes|1\rangle\otimes|1\rangle\otimes|0\rangle^{\otimes(n-2)}$$

$$+\frac{1}{n}\sum_{i=0}^{n-1}|r^{i+1}s\rangle\otimes|r^{(i+1)+l}s\rangle\otimes|0\rangle\otimes|1\rangle\otimes|0\rangle^{\otimes(n-2)}$$

Now all the good cosets have “1” in the second register among the last n registers.

Step 4: Repeat steps 3–4 with new values for i until the last unitary applied was U_m, for some m. This creates mn good cosets. Then measure the last register with respect to the standard basis.

Since after m pairs of steps, there are mn good cosets and each of these corresponds to a 1 in the last register, the probability of measuring the last register with respect to the standard basis and observing 1 is $p = \frac{mn}{n^2} = \frac{m}{n}$. If we obtain 1, then the remaining state is a sum of terms $|\psi\rangle \otimes |a\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes (\mathbb{C}^2)^{\otimes(n-1)}$ such that each $|\psi\rangle$ is good coset of H. Therefore, measuring $|\psi\rangle$ with respect to the basis $r^j \otimes r^k s$ will yield, with certainty, a good coset tensor, and we can read the value of l, and hence know the subgroup H, from the outcome of the measurement.

Therefore, this algorithm succeeds with probability $p = \frac{m}{n}$. Let us analyze its complexity. Suppose we choose $m = n$; then we apply the unitary U_{r_i} approximately $n - 1$ times, and U_i approximately n times. Thus, we will need to call the hidden function n times, which makes this algorithm inefficient.

Nevertheless, this algorithm displays a new approach of considering coset states as tensor products of coset elements rather than a superposition of the coset elements.

Bibliography

[1] D. Bacon, A.M. Childs, W. van Dam, Optimal measurements for the dihedral hidden subgroup problem, *Chicago Journal of Theoretical Computer Science*, Article 2, 25 pp., 2006.

[2] D. J. Bernstein, S. Jeffery, T. Lange, A. Meurer, Quantum Algorithms for the Subset-Sum Problem, *Post-Quantum Cryptography*, p.16-33, 2013.

[3] A. Childs, Lecture Notes on Quantum Algorithms, online resource last accessed February 2021, https://www.cs.umd.edu/∼amchilds/qa/qa.pdf, 2021.

[4] K. Conrad, Characters of finite abelian groups, online resource, https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf, last accessed February 2021.

[5] M. Ettinger, P. Høyer, On quantum algorithms for noncommutative hidden subgroups, *Advances in Applied Mathematics 25*, no. 3, 239-251., 2000.

[6] M. Ettinger, P. Høyer, The quantum query complexity of the hidden subgroup problem is polynomial, *Information Processing Letters 91*, no. 1, 43-48., 2004.

[7] J. L. Fernandez, P. Fernandez, On the probability distribution of the gcd and lcm of r-tuples of integers, ArXiv:1305.0536v1, 2013.

[8] J. A. Gallian, Contemporary Abstract Algebra, Eighth edition, Brooks/Cole Cengage Learning, 2013.

[9] M. Grigni, L.J Schulman, M. Vazirani, U. Vazirani, Quantum mechanical algorithms for the nonabelian hidden subgroup problem, *Combinatorica. An International Journal on Combinatorics and the Theory of Computing 24*, no. 1, 137-154., 2004.

[10] A. Helm, A. May, Subset sum quantumly in 1.17^n, *13th Conference on the Theory of Quantum Computation, Communication and Cryptography, Art. No. 5*, 15 pp., 2018.

[11] K. Horan, D. Kahrobaei, The Hidden Subgroup Problem and Post-quantum Group-Based Cryptography, *Mathematical software - ICMS 2018*, 218-226. Lecture Notes in Computer Science, vol 10931. Springer, Cham. 2018.

[12] Y. Inui, F. Le Gall, Efficient quantum algorithms for the hidden subgroup problem over semi-direct product groups, *Quantum Information & Computation 7*, no. 5-6, 559-570., 2007.

[13] G. Ivanyos, F. Magniez, M. Santha, Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem, Quantum Computing, *International Journal of Foundations of Computer Science 14*, no. 5, 723-739., 2003.

[14] G. Kuperberg, A subexponential-time quantum algorithm for the dihedral hidden subgroup problem, *SIAM Journal on Computing 35*, no. 1, 170-188., 2005.

[15] G. Kuperberg, Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem, *8th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 20-34, 2013.

[16] Y. Li, H. Li, A New Quantum Algorithm for the Random Subset Sum Problem, ArXiv: abs/1912.09264, 2019.

[17] C. Lomont, The hidden subgroup problem - review and open problems. ArXiv: quant-ph/0411037, 2004.

[18] C. Moore, A. Russell, L.J. Schulman, The symmetric group defies strong Fourier sampling, *SIAM J. Comput.*, 37(6): 1842-1864., 2008.

[19] M. A. Nielsen , I. L. Chuang Quantum Computation and Quantum Information, Cambridge University Press, ISBN:978-1-107-00217-3.

[20] O. Regev, Quantum computation and lattice problems, *SIAM Journal on Computing 33*, no. 3, 738-760., 2004.

[21] O. Regev, A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space, ArXiv: Quantum Physics, 2004.

[22] M. Roetteler, Quantum algorithms for abelian difference sets and applications to dihedral hidden subgroups, *11th Conference on the Theory of Quantum Computation, Communication and Cryptography*, Art. No. 8, 16 pp., 2016.

[23] Jean-Pierre Serre, Linear representations of finite groups, Springer-Verlag, New York Inc., 1977.

[24] X. Xu, X. Huang, Z. Li, J. Gao, Z. Jiao, Y. Wang,R. Ren, H.P.Zhang, X, Jin, A Scalable Photonic Computer Solving the Subset Sum Problem, *Science Advances*, Vol. 6, no. 5, eaay5853, 2020.

[25] A. Younes, M. Abdel-Aty, Collapsing a Perfect Superposition to a Chosen Quantum State without Measurement, *PLoS ONE*, 9(8): e103612. doi:10. 1371/journal.pone.0103612, 2014.