# Hidden Subgroup Problem

by


| | |
|---|---|
| Shams Ul Arfeen | sa05169 |
| Syed Muhammad Fasih Hussain | sh05204 |



CS/PHY 314/300

*Quantum Computing*

**Integrated Sciences and Mathematics (iSciM)**

Habib University

Fall 2021

# Contents

# 1. Introduction

Hidden subgroup problem is one of the prominent problems of quantum computing. Simon's problem was necessary to show that quantum computers are able to run exponentially faster as compared to classical computers but these results had no real world implications, on the other hand Shor's period finding algorithm was the much needed break through for quantum computing as it found its applications in cryptography and goes to show that as quantum computers are exponentially faster as compared to the classical computers they can break cryptographic code in efficiently which classical computer just simply can't. Both of the above discussed problems had a black box function $f$ and by making repeated calls to the black box function these problems were solved.

These problems can be reduced to the hidden subgroup problem hence rather that finding polynomial time solution for each of the problems on the quantum computer, finding a polynomial time solution to the hidden subgroup problem can solve all problems that can be reduced to it efficiently. Simon and Shor are just some classical examples, other problems such as graph isomorphism can also be reduced to hidden subgroup problem many fields outside theoretical computer science.

In this report we will first go over some of the basics of group theory that are necessary for problem formulation and walking through its solution, afterward we will formulate the problem statement and what can be known about the subgroup if it exists and how problem like Simon's and Shor's can be reduced down to Hidden Subgroup Problem. Next we will cover the classical solution of Hidden Subgroup Problem which takes exponential amount of time and finally quantum solution of Hidden Subgroup Problem which can solve the problem for Abelian groups in polynomial time. We will describe the method of weak Fourier transforms which is a generalization of the Shor's factoring algorithm and the Simon's hidden string problem. It should be noted however that solving the Hidden Subgroup Problem for an arbitrary group in polynomial time still remains an open problem. We will restrict

ourselves to Abelian groups and show that an efficient quantum algorithm exists that finds the hidden subgroup in $O(log(|G|))$ time with high probability.

# 2. Group Theory

All definitions and examples of this chapter are taken from [5] if not stated other wise.

## 2.1 Groups

A group is defined as a set $G$ of elements having an operation $\circ$ such that it satisfies the following conditions:

i) for each pair $x, y$ of elements of $G$, $x \circ y$ is an element of G (Closure axiom)

$$x \circ y \in G : x, y \in G$$

ii) for all $x, y, z$ i$(x \circ y) \circ z = x \circ (y \circ z)$ (Associativity axiom)

$$(x \circ y) \circ z = x \circ (y \circ z) \in G : x, y, z \in G$$

iii) there is an identity element $e$ in $G$ (Identity axiom)

$$e \in G : \forall g \in G \;\; g \circ e = e \circ g = g$$

iv) for each element $g$ in $G$ there exists an inverse element $g*$ in $G$ (Inverse axiom)

$$\forall g \in G \;\; \exists \, g^* \in G : g \circ g^* = g^* \circ g = e$$

### 2.1.1 Generating Set

A generating set $T$ of a group $G$ is a subset of elements of $G$ such that all the elements of $G$ can be expressed as a combination of elements of $T$ and their inverses under the group operation $\circ$. If $T$ generates $G$ then we can write it as $G = \langle T \rangle$. A finitely generated group is a group which is spanned by a finite generating set and if such a group $G$ also has finite cardinality, denoted as $|G|$, it is called a finite group. The order of an element is the cardinality of the set spanned by that element.

### 2.1.2 Abelian Group

If the operation $\circ$ of a group $G$ is commutative ($\forall x, y \in G : x \circ y = y \circ x$) then the group is called an Abelian group. Abelian groups that have only one generating element are called cyclic groups. Group of $n$th roots of unity under multiplication and additive group of integers modulo $n$, $(Z/nZ)^+$, are examples of cyclic groups. This follows from the fact that a primitive $n$th root of unity generates all other $n$th roots while each integer coprime to $n$ is a generating element of $(Z/nZ)^+$.

### 2.1.3 Example

The set of all possible rotational symmetries of a regular hexagon is:

$$\{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$$

with the operation defined on the set being addition module 360° as shown in Figure 2.1. Now if we pick any two elements from the set their sum will always be part of the set hence satisfying the closure theorem. Addition is an associative operation so it satisfies associativity axiom as well. Next the identity element for addition operation is 0° which satisfies the identity axiom. Now if we pick any element of the set the there will always be another element in the set such that their sum is 0°, for example the inverse of 60° is 300° hence the inverse axiom is also satisfied. As all axioms are satisfied hence the rotational symmetries of a regular hexagon is a group $G$.

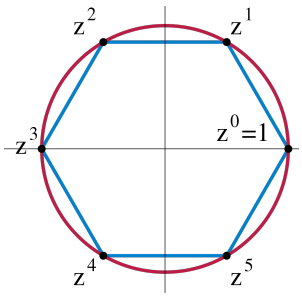


Figure 2.1: Rotational symmetries of a regular hexagon [2]

As the addition operation is commutative hence the $G$ is abelian. All the elements of the $G$ are multiples of 60° hence the generating set of rotational symmetries of a regular hexagon is $\{60^\circ\}$.

## 2.2 Subgroup

Let $H$ be a subset of group $G$ having the same operation $\circ$ as group $G$, $H$ will be a subgroup of $G$ if it satisfies all the requirements of a group stated previously. One observation about $H$ that can be made if it is a subgroup of $G$ is the $H$ will always have the identity element $e$ of $G$ otherwise it will not satisfy the inverse axiom and can't be a group. Based on the previous observations we can say that any group $G$ can not have more that 1 disjoint subgroups as each subgroup of $G$ must have the identity element of $G$ as well.

Every group will always have two possible subgroups, $G$ and $\{e\}$ where $e$ is the identity element of group $G$. Hence, no group can have 2 or more disjoint subgroups.

### 2.2.1 Example

Let $H$ be the group of all possible rotational symmetries of an equilateral triangle with operation addition modulo 360°. The elements in $H$ are $\{0°, 120°, 240°\}$, as all the elements of $H$ are in $G$ and $H$ is also a group under addition modulo 360° hence $H$ is a subgroup of $G$. $H$ has the identity element of $G$ inside it as well.

## 2.3 Coset

Let $H$ be a subgroup of $G$ and $g$ be any element of group $G$ then the left coset of $gH$ will be the set of elements:

$$g \circ H = \{g \circ h : h \in H\}$$

Right coset can also be defined in the same way as we defined the left coset of a subgroup. The right and left cosets of $H$, a subgroup of $G$ will not be equal if $G$ is not abelian.

### 2.3.1 Example

Take $G$ and $H$ from the previous examples and let $g = 60°$, then:

$$g + H = 60° + \{0°, 120°, 240°\}$$

$$g + H = \{60°, 180°, 300°\}$$

As $G$ is closed under addition module 360° then all elements of $g + H$ belong to $G$.

## 2.4 Direct Summation

The direct sum of two groups, $H_1$ and $H_2$ defined over the same binary operation $\circ$, is defined to be the group $G = H_1 \oplus H_2$ which is spanned by the union of the generating sets of two groups [4]. Individual $H_i$ must meet following conditions for $G = \bigoplus_i H_i$ to be defined:

- $H_i \cap H_j = \{e\}$ $(i \neq j)$ where $e$ is identity under the $\circ$ operation.
- $g \circ h \circ g^{-1} \in H_i$ must be true for all $g \in G$ and $h \in H_i$. This is implied for Abelian groups.

### 2.4.1 Example

Let $H_1$ and $H_2$ be rotational symmetries of a line and an equilateral triangle respectively:

$$H_1 = \{0^\circ, 180^\circ\}$$

$$H_2 = \{0^\circ, 120^\circ, 240^\circ\}$$

$H_1 \oplus H_2$ will have elements $\forall h_1 \in H_1 \; \forall h_2 \in H_2 : h_1 + h_2$ as the operation defined over $H_1$ and $H_2$ is addition modulo 360°.

$$H_1 \oplus H_2 = \{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$$

## 2.5 Group Isomorphism

Two groups, $(G, *)$ and $(H, +)$, are said to be homomorphic if there exists a function $f : G \to H$ such that for all $g_1, g_2 \in G$:

$$f(g_1) + f(g_2) = f(g_1 * g_2)$$

Furthermore, if $f$ is bijective, then the two groups are said to be isomorphic.

### 2.5.1 Example

For example, the group $(Z/nZ)^+$ and the group of $n$th roots of unity under multiplication are well-known isomorphic groups. This follows from the fact that when two $n$th roots of unity are multiplied, written as a power of a primitive root, the powers are simply added mod $n$.

# 3. Hidden Subgroup Problem

In this section, we will provide an elegant representation theory that allows us to capture group operations in binary information. Then building on this theory, we will show the standard method for finding the subgroups in Abelian case merely by applying Fourier transform over finite groups. Formally, the HSP problem asks the following:

## 3.1 Problem Statement

"Given a group $G$ and a black box function $f : G \to X$ where $X$ can be any set and $H$ is a subgroup of $G$ such that $f(g_1) = f(g_2)$ iff $g_1H = g_2H$ for all $g_1, g_2 \in G$, find $H$ using the information gained from evaluations of $f$." [8][9]

The finite Abelian HSP problem is a special case of HSP problem when the group $G$ is both finite and Abelian. It can be shown that the well known Simon's algorithm and Shor's algorithms for factoring integers reduce to specific cases of this problem. We now introduce the following two theorems which are important results to analyze the efficient Quantum solution of finite Abelian HSP.

## 3.2 Lagrange's Theorem

Let $G$ be a group with finite number of elements and let $H$ be an subgroup of $G$. Then the number $r$ of distinct left cosets of $H$ in $G$ is equal to $|G|/|H|$ [1].

One thing to note that is Lagrange's theorem only provides the condition that each subgroup must follow, for example if $|G| = 12$ then the possible factors of $|G|$ are $\{1, 2, 3, 4, 6, 12\}$ but that doesn't mean that a subgroup of each of these sizes

must exist, Lagrange's theorem only says that if a subgroup exist then it will be one of these sizes.

### 3.2.1 Proof

Assume that group $G$ has a subgroup $H$, $|H|$ can be divided into 3 possible cases:

1. If $H = \{e\}$ then $|H| = 1$ and 1 divides $|G|$.
2. If $H = G$ then $|H| = |G|$ and $|G|$ divides $|G|$.
3. If $H < G$ and $H \neq \{e\}$. Now to divide the group $G$ into as many possible left cosets as possible. Pick $g_1 \in G : g_1 \notin H$ so this coset will be:

   $$g_1 \circ H = \{g_1 \circ h : \forall h \in H\}$$

   By the construction of $g_1 \circ H$ we can say that $H \cap g_1 \circ H = \emptyset$.

   Assume that $H \cap g_1 \circ H \neq \emptyset$ and there is an element in both $H$ and $g_1 \circ H$:

   $$g_1 \circ h_i = h_j : h_i, h_j \in H$$

   Performing operation $\circ$ with $h_i^{-1}$ on both sides

   $$(g_1 \circ h_i) \circ h_i^{-1} = h_j \circ h_i^{-1}$$

   $$g_1 \circ (h_i \circ h_i^{-1}) = h_j \circ h_i^{-1}$$

   $$g_1 \circ e = h_j \circ h_i^{-1}$$

   $$g_1 = h_j \circ h_i^{-1}$$

   But if $g_1 = h_j \circ h_i^{-1}$ then $g_1 \in H$ and by construction $g_1 \notin H$ hence there is not common element between $H$ and $g_1 \circ H$.

   Pick $g_2 \in G : g_2 \notin H \cup g_1 \circ H$ so this coset will be:

   $$g_2 \circ H = \{g_2 \circ h : \forall h \in H\}$$

   By the construction of $g_2 \circ H$ we can say that $(H \cup g_1 \circ H) \cap g_2 \circ H = \emptyset$. By the same argument as before we can show that $H \cap g_2 \circ H = \emptyset$.

   Assume that $g_1 \circ H \cap g_2 \circ H \neq \emptyset$ and there is an element in both $g_1 \circ H$ and $g_2 \circ H$:

   $$g_1 \circ h_i = g_2 \circ h_j : h_i, h_j \in H$$

Performing operation $\circ$ with $h_j^{-1}$ on both sides

$$(g_1 \circ h_i) \circ h_j^{-1} = (g_2 \circ h_j) \circ h_j^{-1}$$

$$(g_1 \circ h_i) \circ h_j^{-1} = g_2 \circ e$$

$$g_1 \circ h_i \circ h_j^{-1} = g_2$$

But if $g_2 = g_1 \circ h_i \circ h_j^{-1}$ then $h_i \circ h_j^{-1}$ should belong to $H$ hence $g_1 \circ h_i \circ h_j^{-1}$ should belong to $g_1 \circ H$ which is incorrect by the construction of $g_2$ hence $g_1 \circ H \cap g_2 \circ H = \emptyset$.

As $H \cap g_2 \circ H = \emptyset$ and $g_1 \circ H \cap g_2 \circ H = \emptyset$ then $(H \cup g_1 \circ H) \cap g_2 \circ H = \emptyset$.

In the same way we selected $g_2$ we will keep partitioning the group $G$ until all the elements are present inside one of the partitions. Assume we partitioned $G$ into $n+1$ partitions; $H, g_1 \circ H, g_2 \circ H, ..., g_n \circ H$. All of the cosets are disjoint and shouldn't have duplicates.

Assume that $g \circ H$ for some $g \in G$ has duplicates, such that $g \circ h_i = g \circ h_j$ for some $h_i, h_j \in H$. Performing operation $\circ$ with $g^{-1}$ on both sides:

$$g^{-1} \circ (g \circ h_i) = g^{-1} \circ (g \circ h_j)$$

$$h_i = h_j$$

This is only possible if $h_i = h_j$ hence there are no duplicates in $g \circ H$ as there are no duplicates in $H$.

As there are $n+1$ partitions of $G$ each of size $|H|$ so we can say that:

$$|G| = (n+1) \times |H|$$

Hence $|G|$ is divisible by $|H|$. Proof taken from [1].

## 3.3 Fundamental Theorem of Finite Abelian Groups

This theorem states that every finite Abelian group $G$ is isomorphic to a direct sum of cyclic groups of prime power order, written as:

$$G \cong \bigoplus_{i=0}^{u} (Z/k_i Z)^+$$

Where all $k_1, k_2 ... k_u$ are powers of prime numbers not necessarily distinct.

### 3.3.1 Proof

Let $G$ be the finite Abelian group under consideration, then:

1. Since $G$ is a finite group, it is also finitely generated.
2. Let $T = \{t_i\}$ be the generating set of $G$. Then every element $g \in G$ can be written as combinations of the basis $\{t_i\}$.
3. Let $H_i$ be the cyclic subgroup of $G$ generated by $t_i$.
4. Then $H_i$ is isomorphic to $(Z/nZ)^+$ where $n = |H_i|$.
5. $(Z/mnZ)^+$ is isomorphic to the direct sum of $(Z/nZ)^+$ and $(Z/mZ)^+$ where $n$ and $m$ are coprime.
6. By previous two statements, each $H_i$ can be decomposed into a direct sum of the form $\bigoplus_i (Z/k_i Z)^+$ so that each $k_i = p_i^{n_i}$ where $p_i$ is a prime number and $n_i$ is an integer.
7. $G$ is a direct sum of all $H_i$.
8. By previous two statements, $G$ is also a direct sum of the form $\bigoplus_i (Z/k_i Z)^+$, where each $k_i$ is a power of prime number not necessarily distinct.

## 3.4 Reduction of Simon's Problem

In this instance $G$ is the set of all binary strings of size $n$ with operation addition defined over them, $f(x) = x \oplus s$ where $s$ is some binary string of size $n$ and $H = \{0, s\}$ hence finding the hidden group will give the value of $s$ [9].

## 3.5 Reduction of Period Finding Problem

Period finding problem finds the smallest value of $r$ if it exists such that $f(r) = 1$. Here $f(x) = a^x \mod N$ and $r$ is the period of $a$ in $\mod N$.

In this case the $G$ is set of integers and $H$ is the set of all possible multiples of $r$, as the nature of function is periodic hence the value of function should remain constant inside each coset i.e. $f$ is constant in the coset $g + H$ for some $g \in G$. The value of $r$ is the smallest element of $H$ [9].

# 4. Classical Solution of HSP

In this section we will present a classical solution for the HSP problem so that it can serve as a benchmark for the quantum solution. A naive classical algorithm could be stated as follows:

- Compute $s_0 = f(e)$ where $e$ is the identity element of $G$.
- Compute $f(g)$ for all $g \in G$ and return those for which $f(g) = s_0$. This is the entire set $H$.

The time complexity of the above algorithm is $O(|G| \times comp(f))$ while an efficient solution should take time polynomial in $O(log(|G|))$ which is also the amount of bits required to represent the entire structure of a group (i.e. by representing a group with $k_i$'s by fundamental theorem). Without loss of generality, one can appreciate the fact that not all elements are required to represent a group. It suffices for the answer if one can arrive with just the basis of subgroup, that is, its generating set. In fact, there is always a set of size $log(|H|) \geq log(|G|)$ that generates $H$. So to optimize our naive algorithm, we shall use an important theorem which states that if one randomly picks $t + log(|H|)$ elements of $H$ then the probability that the obtained set generates $H$ is greater than $1 - 2^{-t}$ as shown in [3]. Classically, there is no known probabilistic algorithm to exploit this result.

# 5. Quantum Solution of HSP

Finally, we state the quantum efficient solution of the finite Abelian HSP. Consider the decomposition of the given group $G \cong (Z/k_1Z)^+ \oplus (Z/k_2Z)^+ ... \oplus (Z/k_tZ)^+$ and let $U_f : G \to X$ be the corresponding quantum black box function that hides the subgroup $H$ of $G$. Let $N = \lceil \log(k_1) \rceil + \lceil \log(k_2) \rceil ... + \lceil \log(k_t) \rceil$ be the number of qubits in input register and $M = log(|X|)$ be qubits in the output register. Define the following quantum circuit where we have denoted a $k \times k$ DFT matrix as $F_k$:

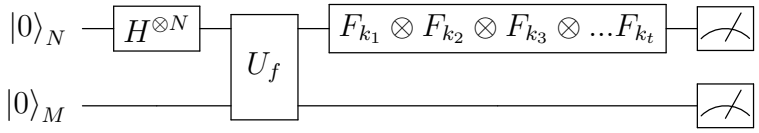


Table 5.1: Quantum circuit for HSP [7]

Note that the first register is a product of $t$ states where a general state is written as $|g\rangle_N = |g_1\rangle_{k\,1} \otimes |g_2\rangle_{k\,2} \otimes ... |g_t\rangle_{k\,t}$. This division is fundamental in all Abelian groups by the fundamental theorem. After applying $U_f$ we have the following state:

$$|0\rangle_N |0\rangle_M \to \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_N |f(g)\rangle_M$$

Assume after measuring the second register on this point we observe the value $f(g_0) = y$, thus our first register is now in the superposition of a certain coset of $H$ i.e. the coset $g_0H$. The state is:

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |h + g_0\rangle$$

Now we apply the final gate $F_G = F_{k1} \oplus F_{k2} ... \oplus F_{kt}$ on this register.

$$F_G \frac{1}{\sqrt{|H|}} \sum_{h \in H} |h + g_0\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} F_G |h + g_0\rangle$$

$$= \frac{1}{\sqrt{|H|.|G|}} \sum_{h \in H} \sum_{g \in G} (\prod_{i=1}^{t} e^{2i\pi \frac{g_i(g_{0i}+h_i)}{k_i}}) |g\rangle$$

$$= \frac{1}{\sqrt{|H|.|G|}} \sum_{h \in H} \sum_{g \in G} X_g(g_0 + h) |g\rangle$$

Where $X_g(g') = \prod_{i=1}^{t} e^{2i\pi \frac{g_i g'_i}{k_i}}$ is a group homomorphism [6]. We note that $X_g(g') = X_{g'}(g)$ and $X_g(g' + g'') = X_g(g')X_g(g'')$. We define a group $H^\perp = \{g \in G | X_g(h) = 1 \forall h \in H\}$. It can be shown that $(H^\perp)^\perp = H$ and furthermore, $H^\perp$ is isomorphic to $G/H$ [6]. Now, we show that by measuring state of first register, we can uniformly sample elements of $H^\perp$. The probability to get any element of $H^\perp$ is:

$$\frac{1}{|H|.|G|} \sum_{g \in H^\perp} \left| X_g(g_0) \sum_{h \in H} X_g(h) \right|^2 = \frac{1}{|H|.|G|} \sum_{g \in H^\perp} |X_g(g_0)|^2 \left| \sum_{h \in H} X_g(h) \right|^2$$

As $X_g(g_0)$ is of the form $e^{i\theta}$ so its mod square is 1 while all terms in the summation $\sum_{h \in H} X_g(h)$ are 1's by definition of $H^\perp$. Recalling that $|H^\perp| = |G|/|H|$ we found that it is guaranteed to get elements of $H^\perp$:

$$= \frac{1}{|H|.|G|} \sum_{g \in H^\perp} |1|^2 \left| \sum_{h \in H} 1 \right|^2$$

$$= \frac{|H^\perp|.|H|^2}{|H|.|G|} = 1$$

### 5.0.1 Classical Post-Processing

For each element of $H^\perp$ that one samples, one can write a linear congruence with elements of $H$. Consider for example $X_g(h) = 1 = \prod_{i=0}^{t} e^{2i\pi \frac{h_i g_i}{t_i}}$ and assume $\gamma$ as the lowest common multiple of $t_i$'s then equation implies:

$$\sum_{i}^{t} \gamma h_i g_i / t_i \cong 0 \ \textbf{Mod} \ \gamma$$

The above equation can be converted to Smith normal form to get linear congruences of the form $ah = b$ **Mod** $\gamma$ whose solution can be enumerated by well known methods [7]. Repeating the entire procedure about $O(log|G|)$ times gives a generating set of $H$ with high probability. Thus, we have completed proof of correction of the algorithm.

# 6. Conclusion and Future Work

We showed how isomorphism in Abelian groups allows us to find hidden subgroups by using representation in terms of additive integer modulo groups. We stated the theorem describing how finite groups are built from simple cyclic groups using summation series. We described the standard method to solve finite Abelian HSP problem by gathering information on the hidden subgroup from coset states i.e. uniform superposition over a random coset of H. By taking credits from previous works, we proved that the problem lies in BQP class. We also indicated how HSP reduces to various efficient quantum algorithms such as Shor's factoring algorithm and Simon's period finding algorithm. The work can be extended to show that the provided generalization of the Fourier transform is enough to solve Dedekindian Hidden Subgroup Problem for which the hidden subgroup is invariant under conjugation i.e. $g \circ h \circ g^{-1} \in H$ for all $h \in H$ and $g \in G$. An extension to the non-abelian case can be shown by defining a Quantum Fourier Transform over finite groups using the generalization of strong Fourier sampling. This is done by replacing the initial Hadamard gate by a general gate $V$. This generalization has been shown in the famous work by Mark Ettinger and Peter Høyer [3].

# References


[1] *Cosets and Lagrange's Theorem - The Size of Subgroups (Abstract Algebra)*. May 2017. URL: https://youtu.be/TCcSZEL_3CQ.

[2] *Cyclic group*. URL: https://en.wikipedia.org/wiki/Cyclic_group.

[3] Mark Ettinger and Peter Høyer. *On Quantum Algorithms for Noncommutative Hidden Subgroups*. 1998.

[4] *Group Direct Sum*. URL: https://mathworld.wolfram.com/GroupDirectSum.html.

[5] J.F. Humphreys et al. *A Course in Group Theory*. Oxford Graduate Texts in Mathematics. Oxford University Press, 1996. ISBN: 9780198534594. URL: https://books.google.com.pk/books?id=2jBqvVb0Q-A.

[6] Chris Lomont. *The Hidden Subgroup Problem Review and Open Problems*. 2004.

[7] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 2007.

[8] Ryan O'Donnell and John Wright. *Quantum Computation and Information*. 2015. URL: https://www.cs.cmu.edu/~odonnell/quantum15/.

[9] Ronald de Wolf. *Quantum Computing: Lecture Notes*. 2021. arXiv: 1907.09415 [quant-ph].