

The Hidden Subgroup Problem

River McCubbin With Supervisor Camelia Karimian-Pour

October 26, 2023

Overview

1. History and Background:
 - 1.1 Linear Algebra
 - 1.2 Group Theory
 - 1.3 Quantum Computing
 - 1.4 Representation Theory
 - 1.5 Quantum Fourier Transform
2. Abelian HSP
3. Non-Abelian HSP

Linear Algebra: Hilbert Space

Definition (Hilbert Space)

A vector space \mathcal{H} is called a *Hilbert space* if it is a complete inner product space, i.e. a vector space with an inner product such that any Cauchy sequence in \mathcal{H} converges in \mathcal{H} with respect to the inner product.

Typically \mathbb{C}^{2^n} .

Linear Algebra: Operators

Definition (Linear Operator)

A *linear operator* $\phi : V \rightarrow W$ between two vector spaces over a field \mathbb{F} is an operator satisfying $\phi(ax + by) = a\phi(x) + b\phi(y)$, for all $x, y \in V$ and $a, b \in \mathbb{F}$.

Definition (Adjoint Operator)

Given an operator $\phi : \mathcal{H} \rightarrow \mathcal{H}$ on a Hilbert space \mathcal{H} , we define the *adjoint* operator ϕ^* such that $\langle \phi(x), y \rangle = \langle x, \phi^*(y) \rangle$.

If ϕ has a complex matrix representation T then we can find the matrix representation of ϕ^* by taking the conjugate transpose of T , denoted T^* .

Definition (Unitary Operator)

A linear operator $U : \mathcal{H} \rightarrow \mathcal{H}$ on a Hilbert space \mathcal{H} is called *unitary* if it preserves the inner product and hence the norm, i.e. if it satisfies $\langle U(x), U(y) \rangle = \langle x, y \rangle$.

Group Theory: Groups


Definition (Group)

A *group* $G = (X, \cdot)$ is a set of elements X along with an operation \cdot on X , such that the following properties hold:¹

- ▶ There exists an element $e \in G$ such that $ae = ea = a$. This element is called the *identity* element.
- ▶ $\forall a, b \in G$ we have that $ab \in G$.
- ▶ $\forall a, b, c \in G$ we have that $(ab)c = a(bc)$.
- ▶ $\forall a \in G, \exists a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

Finite groups only!

Order = Size

¹the \cdot is often omitted as concatenation, $a \cdot b = ab$ 

Group Theory: Subgroups

Definition (Subgroup)

A *subgroup* $H = (A, \cdot)$ of a group $G = (B, \cdot)$ is a group with the same operation as G but fewer elements, $A \subseteq B$. If H is a subgroup of G then we write $H \leq G$ if it may be equal, and $H < G$ if $H \neq G$.

Definition (Coset)

A *coset* of a subgroup $H \leq G$ is the set $a \cdot H = \{a \cdot h \mid h \in H\}$. If G is non-abelian then we differentiate the *left* coset as defined above, and the *right* coset $Ha = \{h \cdot a \mid h \in H\}$.

Group Theory: Generating Groups

Definition (Generating Set)

A *generating set* for a group G is a set of elements $\langle g_1, g_2, \dots, g_n \rangle$ such that any element of G can be expressed as a combination of g_i .

Example: $\mathbb{Z}_3 = \langle 1 \mid 3 = 0 \rangle$.

Group Theory: Classifying Groups

Definition (Cyclic Group)

A group G is called *cyclic* if

$G = \{e, g, g^2, g^3 \dots g^{n-1}\} = \langle g \mid g^n = e \rangle$ for some element $g \in G$. We denote such a group C_n where n is the number of elements in G .

Definition (Dihedral Group)

A group G is called a *dihedral group* if

$G = \{e, r, r^2 \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\} = \langle r, s \mid r^n = s^2 = srsr = e \rangle$. We denote the dihedral group of size $2n$ as D_n or D_{2n} .

This notation varies by author, and is typically clearly illustrated due to the prevalence of both of these notations. For this report, we will be using the notation D_{2n} to represent the dihedral group of size $2n$. The dihedral group of size $2n$ represents the symmetries of a regular n -gon.

Group Theory: Morphisms on Groups

Definition (Homomorphism)

A function $f : G \rightarrow K$ between groups G and K is called a *homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Definition (Isomorphism)

A function $f : G \rightarrow K$ between groups G and K is called an *isomorphism* if f is a bijective homomorphism. If such a map exists then we say that G is *isomorphic* to K and we write $G \cong K$.

Quantum Computing: Terminology

Definition (Computational Basis)

The *computational basis* is an orthonormal basis for \mathcal{H} , and is assumed to be equivalent to the standard basis unless stated otherwise.

Definition (Qubit)

A *qubit* is a unit vector in \mathbb{C}^n , i.e. a vector with length 1.

For example, in \mathbb{C}^2 we take $\mathcal{B} = \{|0\rangle = (1, 0), |1\rangle = (0, 1)\}$ to be the computational basis.

Quantum Computing: Tensor Products I

Definition (Tensor Product of Vectors)

Let V and W be two vector spaces with bases \mathcal{B}_V and \mathcal{B}_W respectively, both over a field \mathbb{F} . Given

$$v = \sum_{v_i \in \mathcal{B}_V} a_i v_i \in V$$

and

$$w = \sum_{w_j \in \mathcal{B}_W} b_j w_j \in W$$

with $a_i, b_j \in \mathbb{F}$, we define the *tensor product*

$$v \otimes w = \sum_{v_i \in \mathcal{B}_V} \sum_{w_j \in \mathcal{B}_W} (a_i b_j) (v_i \otimes w_j)$$

where $(v_i \otimes w_j)$ is notation for a basis vector in $V \otimes W$.

Quantum Computing: Tensor Products II

Definition (Tensor Product of Vector Spaces)

Let V and W be two vector spaces, both over a field \mathbb{F} . We define $V \otimes W$ as the space generated by all linear combinations of elements $v \otimes w$ with $v \in V$ and $w \in W$.

WARNING: Not all elements are of the form $v \otimes w$.

Definition (Separable and Entangled States)

If an element $a \in V \otimes W$ can be written as $v \otimes w$ for some $v \in V$ and $w \in W$ then we say that a is a *separable* state, otherwise we say that it is an *entangled* state.

As an example of generating larger spaces, in a two-qubit system we generate the computational basis by taking

$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$.

Quantum Computing: More Notation

Since this operation is so common in quantum computing, we often abbreviate this notation as follows: $|ab\rangle := |a\rangle \otimes |b\rangle$. We further simplify this for computational basis vectors, where we denote the first basis vector (the vector with a 1 in the first position and 0s elsewhere) as $|0\rangle$, regardless of the dimension of the space. We denote the second basis vector as $|1\rangle$, the third as $|2\rangle$, and in general the n th basis vector as $|n-1\rangle$.

Quantum Computing: Larger Spaces

Theorem

$$\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n} = \mathbb{C}^{2^{2n}}.$$

Proof.

We can prove this by verifying that the set of pairwise tensor products of basis elements for \mathbb{C}^{2^n} generates a basis for $\mathbb{C}^{2^{2n}}$. We give here a simple example, as the general proof requires knowledge of functional analysis beyond the scope of this report.

Consider the computational basis $\mathcal{B} = \{|0\rangle, |1\rangle\}$ for \mathbb{C}^2 .

We will increase the dimension of our state space by taking $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$.

Computing taking the tensors of our basis we find:

$$|0\rangle \otimes |0\rangle$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix}$$

$$|0\rangle \otimes |1\rangle$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix}$$

Quantum Computing: Bra-Ket Notation

In quantum computing, we represent states by column vectors, denoted by the “ket” symbol $|\psi\rangle$ (read “ket psi”). We use the “bra” symbol $\langle\psi|$ (read “bra psi”) to denote the linear operator $\langle\psi| : \mathcal{H} \rightarrow \mathbb{C}$, the adjoint of $|\psi\rangle$. In essence, this notation is simply a convenient way of writing column vectors ($|\psi\rangle$) and row vectors ($\langle\psi|$). This notation may seem odd, but when put together we can see why it is useful; $\langle\psi||\phi\rangle = \langle\psi|\phi\rangle$ denotes the result of ϕ under the map ψ , which is conveniently given by their inner product $\langle\psi, \phi\rangle$.

Quantum Computing: State Vectors

Definition (State Vector)

A *state vector* $|\psi\rangle \in \mathbb{C}^{2^n}$ is a 2^n -dimensional unit vector where n is the number of qubits in the system. It represents the state of all qubits in the system, and is given by $|\psi\rangle = a|0\rangle + b|1\rangle + \cdots + c|2^n - 1\rangle$.

Definition (Superposition)

If a given state vector is not aligned with a basis vector then we say that this vector is a *superposition*.

Quantum Computing: How to Compute

In order to compute we apply operations to our state. As mentioned, we require that a state be represented by a unit vector; in order to progress from one state to the next, we will require that any operations output only unit vectors. Such operations within a vector space such as \mathbb{C}^{2^n} are called unitary operators, as described in 3. These unitary operators can be applied to act as logical operations, called “logic gates” in the language of computer science. Using these logic gates we can create quantum circuits that are similar to classical circuits, allowing us to perform logical operations such as AND, OR, NOT etc.

Quantum Computing: Sample Computation

For example, we can construct the quantum equivalent of the NOT gate, called the Pauli-X gate. This gate is given by the following matrix:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We can verify that this in fact negates a given qubit:

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \quad &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned}$$

You may notice that this is in fact a rotation matrix, particularly about the X -axis, hence the name Pauli-X gate. There are corresponding Pauli-Y and Z gates that represent rotations about other axes.

Quantum Computing: Limitations

Unfortunately, though, it is not possible to create a universal gate, such as NAND, or NOR. This means that for quantum computation, most circuits need to be designed specifically for the operations we want to run.

Quantum Computing: Measurement

Once we have completed the computation we desire by applying unitary operators, we require a way of measuring the system in order to retrieve the information we have computed. Due to the nature of quantum computing, we cannot directly observe our data. In order to retrieve the information we desire, we require a separable quantum state. Given a separable state, we can retrieve information by applying special operators called *measurement operators*, which will “collapse” a state in superposition to a basis vector which we can observe.

Definition (Measurement Operators)

A collection $\{M_m\}$ of *measurement operators* is a set of operators satisfying

$$\sum_m M_m^* M_m = I.$$

These operators act on the state space, where the index m represents the measurement outcomes that could occur. If the state of the system before measurement is ψ , then the probability result m occurs is given by

Quantum Computing: Measurement Example

Example

An example of a set of measurement operators is the set of projection matrices in \mathbb{C}^2 . These matrices are given by

$$P_x = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

and

$$P_y = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

It is clear that the sum of these matrices gives back the identity matrix, hence they satisfy the requirement given in the definition of measurement operators.

Since these are projection matrices, it is also evident that after applying these matrices to a vector we obtain a unit vector, satisfying the need to collapse a superposition.

Representation Theory of Groups: Motivation

We continue our necessary background with an introduction to representation and character theory. The discussion of this topic provides the foundation for the Quantum Fourier Transform (QFT). QFT is the key component in algorithms such as Shor's algorithm, famously developed in 1994 to find the prime factors of a given integer efficiently on a quantum computer of sufficient size. Similarly, QFT permits quantum computing to solve problems such as the hidden subgroup problem more efficiently than classical computers.

Representation Theory: Representations

To begin, we define the concept of a *representation* of a group G .

Definition (Representation)

A representation ρ of a group G is a homomorphism $\rho : G \rightarrow GL(V)$ for some finite dimensional vector space V . Here, $GL(V)$ denotes the general linear group of the vector space V , which is the set of invertible matrices on V .

Representation Theory: Characters

We think of a representation as a map that treats group elements of G as functions acting on V . For any given representation, we have an associated *character*.

Definition (Character)

Given a group G with a representation $\rho : G \rightarrow GL(V)$, we define the *character* χ_ρ ² of ρ as the map $\chi_\rho : G \rightarrow \mathbb{C}$ given by $\chi_\rho(g) = \text{tr}(\rho(g))$.

We call this the character of a representation because it carries essential information about the representation and can be used to *characterize* a representation more concisely.

²often the subscript is omitted when there is no room for confusion as to which representation this character is from

Representation Theory: Inner Product

We define an inner product on functions on G by

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

With this inner product we have a sense of orthogonality for characters and other functions on G .

Representation Theory: Isomorphic Representations

Definition (Isomorphic Representations)

Two representations $\rho_1 : G \rightarrow GL(V)$, $\rho_2 : G \rightarrow GL(W)$ of a group G are called *isomorphic*³ if there exists an isomorphism

$\phi : V \rightarrow W$ such that

$\phi(\rho_1(g)(v)) = \rho_2(g)(\phi(v)), \forall v \in V, \forall g \in G$. We write $\rho_1 \cong \rho_2$.

This definition provides us a tool for examining and comparing representations.

³the term “equivalent” is also frequently used

Representation Theory: Irreducible Representations

Definition (Irreducible Representation)

A representation is said to be *irreducible* if there are no non-trivial subspaces $W \subset V$ such that $\rho(g)(W) \subset W, \forall g \in G$. The character of an irreducible representation is called an *irreducible character*.

We can more easily determine if a representation is irreducible by applying the following theorem:

Theorem

A representation ρ is irreducible iff its character χ has norm 1.

Representation Theory: Schur's Lemma I

Theorem (Schur's Lemma)

Let G be a group with irreducible representations $\rho_1 : G \rightarrow GL(V)$ and $\rho_2 : G \rightarrow GL(W)$. Let $f : GL(V) \rightarrow GL(W)$ be a linear operator satisfying $\rho_2(f(g)) = f(\rho_1(g))$. Then we have the following:

- 1. If ρ_1 and ρ_2 are not isomorphic then $f = 0$.*
- 2. If $V \cong W$ and $\rho_1 \cong \rho_2$ then f is a scalar multiple of the identity.*

Representation Theory: Schur's Lemma II

Theorem (Corollary to Schur's Lemma)

If $h : V \rightarrow W$ is a linear operator and h_0 is a map given by

$$h_0 = \frac{1}{|G|} \sum_{g \in G} (\rho_2(g))^{-1} h(\rho_1(g))$$

then:

1. If ρ_1 and ρ_2 are not isomorphic then $h_0 = 0$.
2. If $V \cong W$ and $\rho_1 \cong \rho_2$ then $h_0 = \frac{\text{tr}(h)}{\dim(V)} I$.

Representation Theory: An Orthonormal Set

Theorem

The set of irreducible characters on G , denoted \hat{G} , forms an orthonormal set.

Proof.

We provide an outline of a proof: If χ is the character of an irreducible representation then using the inner product defined by 1 and by 27 we have that $\langle \chi, \chi \rangle = 1$, hence irreducible characters are normal. Using the same inner product, if χ and χ' are the characters of two non-isomorphic irreducible representations then $\langle \chi, \chi' \rangle = 0$. The remainder of the proof of this can be found in [serre]. □

Representation Theory: Conjugate Representation

Definition (Conjugate Representation)

For a representation $\rho : G \rightarrow GL(V)$, the *conjugate representation* $\bar{\rho} : G \rightarrow GL(V^*)$ is given by

$$\bar{\rho}(g) = \overline{\rho(g)}.$$

If ρ has matrix representation A then $\bar{\rho}$ is \bar{A} .

Representation Theory: Conjugate Characters

Theorem

Given a representation ρ , $\chi_{\bar{\rho}} = \overline{\chi_{\rho}}$.

Representation Theory: Irreducible Conjugate Representations

Theorem

The conjugate of an irreducible representation is irreducible.

Proof.

Let $\rho : G \rightarrow GL(V)$ be an irreducible representation with character χ_ρ .

Then:

$$\begin{aligned}\langle \chi_{\bar{\rho}}, \chi_{\bar{\rho}} \rangle &= \langle \overline{\chi_\rho}, \overline{\chi_\rho} \rangle && \text{by 32} \\ &= \langle \chi_\rho, \chi_\rho \rangle && \text{by definition of inner product} \\ &= 1 && \text{by 27 since } \rho \text{ is irreducible}\end{aligned}$$

Hence $\bar{\rho}$ is irreducible by 27. □

Given an irreducible representation, this allows us to easily find another.

Representation Theory: Class Functions

Definition (Class Function)

A function $f : G \rightarrow V$ is called a *class* function if it is constant on conjugacy classes of G , i.e. if $f(hgh^{-1}) = f(g), \forall g, h \in G$.

For abelian groups, these represent all functions on G .

Representation Theory: An Orthonormal Basis

Theorem

For a given group G , the set $\hat{G} = \{\chi_0, \dots, \chi_{N-1}\}$ of all irreducible characters of G forms an orthonormal basis for the space of class function on G .

Proof.

As shown in 30, we know that this set is orthonormal. It remains to show that it forms a basis, i.e. that this set spans $\text{Cl}(G)$.

Let ρ be an irreducible representation of G .

Let $f \in \text{Cl}(G)$ and suppose that it is orthogonal to every irreducible character of G , i.e. it is not in the span of these characters.

We define the map

$$\rho_f = \sum_{g \in G} f(g) \rho(g)$$

from V into itself.

Let $g' \in G$ be arbitrary.

Then:

Representation Theory: Abelian vs. Non-Abelian Bases

Notice that for abelian groups the set of class functions on G , denoted $\text{Cl}(G)$ is equivalent to the set of all complex valued functions on G , \mathbb{C}^G . This fact is important in our construction and application of the Quantum Fourier Transform, as the transform applies a change of basis and this will be the basis we choose. Unfortunately, this is not the case for non-abelian groups, and hence the same construction does not suffice. Instead of using the characters of irreducible representations as an orthonormal basis for the class functions, for non-abelian finite groups we proceed as follows:

Determine the set of all irreducible representations ρ_i of G . We choose a basis \mathcal{B} for each representation such that the matrix $M_\rho(g) = (\rho_{ij}(g))_{i,j}$ is unitary for each $g \in G$. We call the entries of these matrices the matrix coefficients of ρ with respect to the chosen basis \mathcal{B} . These matrix coefficients define functions from $G \rightarrow \mathbb{C}$, and furthermore form an orthogonal basis for \mathbb{C}^G . By normalizing we find an orthonormal basis for \mathbb{C}^G . Proof of this can be found in [perepechaenko] and [serre].

The Quantum Fourier Transform: Motivation

With the appropriate background and a basis for \mathbb{C}^G , we can now define the general quantum fourier transform. This transform, as alluded to in 22, is a change of basis formula. In particular, the basis we change to is generated by the irreducible representations of a group G , and is invariant under the group actions of G , i.e. if $|i\rangle$ is a basis vector then $\rho(g)(|i\rangle) \in \text{span}\{|i\rangle\}$.

QFT: Abelian QFT

As mentioned at the end of the previous section, the basis differs based on whether we have an abelian group. For abelian groups, we obtain the formula

$$\mathcal{F}_G(|g\rangle) = \frac{1}{\sqrt{|G|}} \sum_{i=0}^{|G|-1} \chi_i(g) |\chi_i\rangle. \quad (2)$$

using the basis of irreducible characters of G , which is an orthonormal basis for \mathbb{C}^G by 35.

QFT: Non-Abelian QFT

For general non-abelian groups we recall from that the set of irreducible characters is not a basis for \mathbb{C}^G , but invoking 36 we can use the set of scaled matrix coefficients as a basis, giving the *general Quantum Fourier Transform*:

$$\mathcal{F}_G(|g\rangle) = \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \hat{G}} \sqrt{\dim(\sigma)} \sum_{i,j=1}^{\dim(\sigma)} \sigma(g)_{i,j} |\sigma, i, j\rangle \quad (3)$$

where $|\sigma, i, j\rangle$ denotes the map from $GL(V) \rightarrow \mathbb{Z}$ taking a group element g to it's matrix coefficient at i, j under σ , or more concisely $|\sigma, i, j\rangle(g) = \langle i | \sigma(g) | j \rangle$.

QFT: Equivalent Transforms

Notice that for the case of abelian groups the general QFT is equivalent to that of the abelian QFT; the representations are all of dimension 1 and hence the matrices are 1×1 , meaning that the second sum in the general QFT disappears and we obtain the abelian case. Thanks to this, when we discuss the quantum fourier transform in the future we will discuss only the general case unless stated otherwise.

QFT: QFT is Unitary

Referring back to 10 we recall that any transformation we apply must be unitary. Fortunately for us, QFT is a unitary transform:

Theorem

The quantum fourier transform is a unitary transformation.

Proof.

A formal proof of this can be found in [perepechaenko], but we provide an intuitive argument here. Notice that the general quantum fourier transform is a transformation from an orthonormal basis to an orthonormal basis. This means that, at the very least, \mathcal{F} preserves the norm of unit vectors, which is sufficient for our purposes. □

QFT: Example

This definition can appear intimidating, and so we now examine an example of applying the quantum fourier transform, based on [hadfield].

Example

We consider a simple example using the group \mathbb{Z}_2 and denote the elements of this group by the vectors $|0\rangle$ and $|1\rangle$ and operation given by $|i\rangle + |j\rangle = |i + j \bmod 2\rangle$. The state space we take to be $\mathbb{C}^2 = \mathbb{C}\mathbb{Z}_2$. For this group we have two irreducible representations, given by

$$\rho_0(|i\rangle) = |i\rangle$$

and

$$\rho_1(|i\rangle) = |(-1)^i\rangle$$

with characters

$$\chi_0(|i\rangle) = |i\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} |i\rangle$$

and

$$\chi_1(|i\rangle) = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} |i\rangle$$


HSP: Separating Function

With the background provided, we are now prepared to discuss the main topic of this report, the hidden subgroup problem (HSP). The HSP relies on the concept of a *hiding function* over a group G .

Definition (Separating Function)

We say that a function $f : G \rightarrow X$ mapping a group G to a set X *separates cosets* of a subgroup H if for any $g_1, g_2 \in G$ we have

$$f(g_1) = f(g_2) \iff g_1H = g_2H.$$

HSP: The Problem

With this notion of separating cosets, we can discuss the problem of *hiding* them:

Problem (Hidden Subgroup Problem)

Given a group G , a finite set X and a function $f : G \rightarrow X$ that separates cosets of subgroup H , use evaluations of f to determine a generating set for H .

This problem can be solved classically by evaluating $f(g)$ for every $g \in G$, but this method is incredibly inefficient. Quantum algorithms allow this to be computed much more efficiently, as we will see in 47

Abelian HSP: Introduction

We begin our discussion of the hidden subgroup problem with abelian groups. Abelian groups provide the simplest case of the hidden subgroup problem, since the structure given by the abelian property can be leveraged to simplify the HSP.

Abelian HSP: Example

An example of the Hidden Subgroup Problem over abelian groups is the Discrete Logarithm Problem. The Discrete Logarithm Problem is described as follows:

Problem (Discrete Logarithm Problem)

Given a group $G = \mathbb{Z}_p$ generated by an element g , and an element $h = g^r \in G$, determine r .

To formulate this in terms of the hidden subgroup problem, we first translate from \mathbb{Z}_p to the group $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ with entry-wise multiplication mod p . The subgroup is given by

$H = \{(xr, x) \mid x \in \mathbb{Z}_{p-1}\}$ where r is the exponent $h = g^r$. The function f is given by

$$f(x, y) = g^x h^{-y} = g^x g^{-ry} = g^{x-ry}$$

where g is the generator for G . We now show that H is in fact a subgroup, and that f separates cosets of H .

Theorem

the set $H = \{(xr, x) \mid x \in \mathbb{Z}_{p-1}\}$ is a subgroup of

$\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$

Algorithms for HSP: Coset Sampling Method

The most common method for solving the HSP is the *Coset Sampling Method*.

The coset sampling method is described in [perepechaenko] as follows: Let G be a finite group and H a subgroup hidden by the function $f : G \rightarrow X$. Let \mathcal{H} be a Hilbert space spanned by the elements of X and let \mathcal{G} be the Hilbert space spanned by elements of G .

Note: We use ψ_i to denote the i th state vector of our program. This means that i increases by 1 for each operation applied to our state vector.

Step 1: To begin, we prepare two registers. The first register is given by

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

and contains a uniform superposition of the elements of G . The second register is initialized to $|0\rangle$, and later will store states of \mathcal{H} . Notice that both registers are represented in our state vector ψ_i : the first register is represented by $|g\rangle$ on the

Coset Sampling Method: Example

The theoretical aspect of this method can be complicated, so we proceed with an example:

Example

Let $G = \mathbb{Z}_6$, $H = \{0, 3\}$. We can find the cosets of H are as follows:

$$H = \{0, 3\}$$

$$1 + H = \{1, 4\}$$

$$2 + H = \{2, 5\}$$

We take the hiding function f to take a coset to the smallest element it contains, i.e.

$$f(H) = 0$$

$$f(1 + H) = 1$$

$$f(2 + H) = 2$$

From these definitions we can determine the values mentioned in

Non-Abelian HSP: Dihedral Groups

For the sake of this report, we define

$$D_{2n} = \langle r, s \mid r^n = s^2 = rsrs = e \rangle.$$

Non-Abelian HSP: Subgroups

Theorem

D_{2p} has $p + 3$ subgroups.

Example

As an example, consider D_4 . Notice that $D_4 = D_{2p}$ with $p = 2$, and hence has $2 + 3 = 5$ subgroups, namely

$$\langle e \rangle, \langle r \rangle, \langle s \rangle, \langle rs \rangle, D_4.$$

Given a hiding function f and a hidden subgroup H , we determine H by querying (evaluating f on) e, r, rs .

Let q_1, q_2 denote two queried elements. If $f(q_1) = f(q_2)$ then we have that $q_1, q_2 \in cH$ for some c , and hence $q_1^{-1}q_2 \in H$. Since we queried generators, we have that $q_1^{-1}q_2$ generates H .

If $f(q_1) \neq f(q_2) \neq f(q_3)$ (i.e. they are all distinct) then the cosets of H must separate these elements.

Notice that there is no way to construct cosets of the listed subgroups such that this occurs, other than to separate all elements i.e. H must be the trivial subgroup $\langle e \rangle$.

Non-Abelian HSP: Subgroups of D_{2p}

We can extend this method to any prime dihedral group D_{2p} with $p \neq 2$ by querying $e, r, r^k s$ for $1 \leq k < p$. Formalizing this we have the following theorem:

Theorem

For $G = D_{2p}$ with $p \neq 2$ there exists an algorithm to solve the HSP over G with $\frac{p+5}{2}$ queries.

Non-Abelian HSP: A Method for Solving HSP over D_{2n}

Theorem

If $G = D_{2n}$ and $H \leq G$ be a subgroup hidden by the function $f : G \rightarrow X$. Then $f|_{C_n} : C_n \rightarrow X$ hides $H \cap C_n$.

Proof.

Let $a, b \in C_n$ such that $f(a) = f(b)$.

Then $aH = bH \implies ab^{-1} \in H$.

Since $a, b \in C_n$, by closure we have $ab^{-1} \in C_n$.

Hence $ab^{-1} \in C_n \cap H$.

Suppose $a(H \cap C_n) = b(H \cap C_n)$.

Then $ab^{-1} \in H \cap C_n \implies ab^{-1} \in H$ and $ab^{-1} \in C_n$.

By closure of C_n this gives that $a, b \in C_n$.

Notice that $ab^{-1} \in H \implies ab^{-1}H = H \implies aH = bH$, hence $f(a) = f(b)$.

Therefore $f(a) = f(b) \iff a(H \cap C_n) = b(H \cap C_n)$, as wanted. □

This result permits us to study the dihedral HSP in terms of cyclic groups, meaning that we can apply the coset sampling method and the hidden subgroup algorithm.