The Hidden Subgroup Problem

River McCubbin

Supervisor Camelia Karimian-Pour

August 14, 2023

1 Introduction

To be filled at the end

2 History and Background

In order to ease understanding of this report, we begin with this section discussing the relevant pre-requisite materials and the history of the hidden subgroup problem. These materials include linear algebra with a brief mention of elementary functional analysis, the basics of quantum computing, as well as some theory of groups and group representation theory. The aim of this section is to review and/or introduce these concepts at a level understandable to undergraduate students, with relevant examples to aid with more advanced concepts.

2.1 Linear Algebra

We suppose that a basic understanding of linear algebra is present, i.e. an understanding of vectors and a basic understanding of fields and their operations. With this background, we present the following relevant definitions and theorems:

> **Definition 1** (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.

When discussing quantum computing we work primarily in the space $\mathbb{C}^{2^n}$, which is a finite dimensional complex vector space. As such, we can find a basis for this space. Given a basis, we can denote our vectors as a list of coordinates and to concretely compute operations on our vectors.

We can also interact with vectors via various *operators*. The most common type of operator is a *linear* operator, defined as follows:

> **Definition 2** (Linear Operator)**.**
> A *linear operator* $\phi : V \to W$ 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 $a, b \in \mathbb{F}$.

Linear operators preserve the structure of a vector space, but not necessarily the the inner product, and hence not necessarily a notion of distance (norm). We can refine this definition to a new type of linear operator which does preserve the inner product of a vector space and hence the norm, called a *unitary* operator:

> **Definition 3** (Unitary Operator)**.**
> A linear operator $U : \mathcal{H} \to \mathcal{H}$ on a Hilbert space $\mathcal{H}$ is called *unitary* if it preserves the norm, i.e. if it satisfies $\langle U(x), U(y)\rangle = \langle x, y\rangle$. Another convenient fact about these operators is that they are *self-adjoint*, i.e. they satisfy $UU^* = U^*U = I$ where U^* is the conjugate transpose of U.

These operators provide the foundation of quantum computation, which is what we will see in section 2.3

2.2 Group Theory

The Hidden Subgroup Problem is a problem stated in the language of group theory. We will continue our discussion by going over some preliminary knowledge on groups and their instruction so that we can appropriately understand and discuss the HSP.

> **Definition 4** (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 $aa^{-1} = a^{-1}a = e$.

For this report we will restrict our discussion of groups to *finite* groups. We denote the number of elements, or *order*, of a group as $|G|$. This notation also applies to subgroups. We use the same notation and terminology to denote the order of an element $g \in G$ where $|g| = \min(\{n \mid g^n = e\})$.

For a given group G, we can more concisely denote and classify a group by finding a *generating set* for G.

> **Definition 5** (Generating Set)**.**
> A *generating set* for a group G is a set of elements $\langle g_1, g_2, \ldots, g_n\rangle$ such that any element of G can be expressed as a combination of g_i.

Along with a generating set, we can specify a group by the equations that hold with the group's operation and elements. For example the group of integers modulo 3, $\mathbb{Z}_3 = (\{0, 1, 2\}, +_{\mod 3})$, can be expressed as $\langle 1 \mid 3 = 0\rangle$. This *generator expression* completely characterises this group; it contains all of the relevant information to distinguish this group from any other.

With this way of describing groups we can discuss some particular types of group:

> **Definition 6** (Cyclic Group)**.**
> A group G is called *cyclic* if $G = \{e, g, g^2, g^3 \ldots g^{n-1}\} = \langle g \mid g^n = e\rangle$ for some element $g \in G$. We denote such a group C_n where n is the number of elements in G.

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

Definition 7 (Dihedral Group)**.**
A group G is called a *dihedral group* if $G = \{e, r, r^2 \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\} = \langle r, s \mid r^n = s^2 = srsr = e\rangle$. 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 dihdedral group of size $2n$. The dihedral group of size $2n$ represents the symmetries of a regular n-gon.

In any given group, we can have additional structures within that are not necessarily captured by these classifications. One such example of inner structure is a *subgroup*:

Definition 8 (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 $H \leqslant G$ if it may be equal, and $H < G$ if $H \neq G$.

From subgroups we can generate *cosets*, which will be particularly relevant to the discussion later on:

Definition 9 (Coset)**.**
A *coset* of a subgroup $H \leqslant G$ 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 $Ha = \{h \cdot a \mid h \in H\}$.

We complete our review of group theory with a brief mention of morphisms (functions) on groups.

Definition 10 (Homomorphism)**.**
A function $f : G \to K$ between groups G and K is called a *homomorphism* if $f(ab)f(a)f(b)$ for all $a, b \in G$.

Definition 11 (Isomorphism)**.**
A function $f : G \to K$ between groups G and K is called an *isomorphism* if f is a bijective homomorphism.

These types of functions provide a convenient way of comparing the structure of groups.

2.3 Basics of Quantum Computing

With the appropriate background in linear algebra and group theory, we begin our discussion of quantum computing. The foundation of quantum computing are Hilbert spaces, defined in section 2.1. In the context of quantum computing, we call the Hilbert space in which we work our *state space*. As mentioned in Section 2.1, we typically work with $\mathcal{H} = \mathbb{C}^{2^n}$.

We first introduce some terminology.

Definition 12 (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 13 (Qubit)**.**
A *qubit* is a unit vector in $\mathbb{C}^n$, i.e. a vector with length 1.

These are simply new terms for objects that we have already seen; the computational basis will be the name we give the standard basis and a qubit is the name that we give a unit vector in $\mathbb{C}^n$.

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

Of course, computing on a single qubit is practically useless; we require many bits in order to represent most data of interest. We can construct higher dimensional spaces (spaces with more qubits) by taking

the *tensor product* of smaller spaces. We can extend this further; if we wish to compute on multiple pieces of data we can construct spaces to represent each of them, and take the tensor product of their respective spaces in order to generate a space capable of representing them simultaneously.

Definition 14 (Tensor Product)**.**
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 $V \otimes W$.

For example, in a two-qubit system we generate the computational basis by taking $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$. 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 nth basis vector as $|n-1\rangle$.

We can verify that these tensor product do in fact generate bases for higher dimensions as follows:

Theorem 1. $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n} = \mathbb{C}^{2^{2n}}$.

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:

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

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

which generates a basis for $\mathbb{C}^4$, as wanted. □

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 $\langle\psi| : \mathcal{H} \to \mathbb{C}$, 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 $\langle\psi, \phi\rangle$.

Given a basis, we can then discuss a *state vector*.

> **Definition 15** (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 $|\psi\rangle = a\,|0\rangle + b\,|1\rangle + \cdots + c\,|2^n - 1\rangle$.

With our current knowledge we can construct an n-bit system, and represent a state by a vector in $\mathbb{C}^{2^n}$. We now begin a discussion of actual computation; the above is simply the necessary information to set up our system.

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 Section 2.1. 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. 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:

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

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.

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 custom built for the operations we

want to run. 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. This requires what are called *measurement operators*.

Definition 16 (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

$$p(m) = \langle\psi| M_m^* M_m |\psi\rangle$$

and the state after measurement is given by

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$$

An example of a set of measurement operators is the set of projection matrices in $\mathbb{C}^{2^n}$.

2.4 Representation Theory of Groups

We continue our necessary background with an introduction to representation and character theory. The discussion of this topic is what permits the application of the Quantum Fourier Transform, the algorithm that permits quantum computing to solve problems such as the hidden subgroup problem more efficiently than classical computers. To begin, we define the concept of a *representation* of a group G.

Definition 17 (Representation)**.**
A representation ρ of a group G is a homomorphism $\rho : G \to GL(V)$ for some finite dimensional vector space V. Here, $GL(V)$ denotes the general linear group of the vector space V, the set of invertible matrices on V.

We think of a representation as a map that treats group elements of G as functions acting on V.

Definition 18 (Isomorphic Representations)**.**
Two representations $\rho_1 : G \to GL(V), \rho_2 : G \to GL(W)$ of a group G are called *isomorphic* if there exists an isomorphism $\phi : V \to W$ such that $\phi(\rho_1(g)(v)) = \rho_2(g)(\phi(v)), \forall v \in V, \forall g \in G$.

Definition 19 (Character)**.**
The *character* χ of a representation $\rho : G \to GL(V)$ of a group G is the map $\chi : G \to \mathbb{C}$ given by $\chi(g) = \operatorname{tr}(\rho(g))$.

We define an inner product on functions on G by

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

Definition 20 (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*.

Theorem 2 (Schur's Lemma)**.** *Given irreducible representations of G $\rho_1 : G \to GL(V)$ and $\rho_2 : G \to GL(W)$ then for $\phi : GL(V) \to GL(W)$ satisfying $\rho_2(\phi(g)) = \phi(\rho_1(g))$ we have the following:*

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

Proof. The proof of this is given in [**serre**]. □

Theorem 3 (Corollary to Schur's Lemma)**.** *If $\phi : V \to W$ is a linear map such that*

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

then:

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

Proof. The proof of this is given in [**serre**]. □

Theorem 4. 1. *If χ is the character of an irreducible representation then $\langle \chi, \chi \rangle = 1$.*
2. *If χ and χ' are the characters of two non-isomorphic irreducible representations then $\langle \chi, \chi' \rangle = 0$.*

Proof. The proof of this is given in [**serre**]. □

This effectively tells us that the set of irreducible characters on G, denoted $\hat{G}$, forms an orthonormal set.

Definition 21 (Class Function)**.**
A function $f : G \to V$ is called a *class* function if $f(hgh^{-1}) = f(g)$.

Definition 22 (Conjugate Representation)**.**
For a representation $\rho : G \to GL(V)$, the *dual representation* $\rho^* : G \to GL(V^*)$ is given by

$$\rho^*(g) = \overline{\rho(g^{-1})}.$$

Theorem 5. *The conjugate of an irreducible representation is irreducible.*

Proof. First consider the following:

$$\begin{aligned}
\rho^*(g)\rho^*(h) &= \overline{\rho(g^{-1})\rho(h^{-1})} && \text{by definition 22} \\
&= \overline{\rho(h^{-1})\rho(g^{-1})} && \text{by definition of conjugate} \\
&= \overline{\rho(hg)^{-1}} && \text{since } \rho \text{ is a homomorphism} \\
&= \rho^*(gh).
\end{aligned}$$

This shows that ρ^* is a homomorphism from G to $GL(V^*)$ and hence a representation.
Since eigenvalues are preserved by transpose we have that $\rho(g^{-1})$ and $\rho^*(g)$ have the same eigenvalues.
Since $\chi_{\rho^*}(g) = \mathrm{tr}\,(\rho^*(g))$ we have that it is the sum of eigenvalues of $\rho^*(g) = \rho(g^{-1})$ and hence is an irreducible character, as wanted. □

Theorem 6. *For a given group G, the set $\hat{G} = \{\chi_0 \ldots, \chi_{N-1}\}$ of all irreducible characters of G forms an orthonormal basis for the space of class function on G.*

Proof. As shown in theorem 4, we know that this set is orthonormal. It remains to show that it forms a basis, i.e. that this set spans $\mathrm{Cl}(G)$.

Let ρ be an irreducible representation of G.
Let $f \in \mathrm{Cl}(G)$ 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:

$$\begin{aligned}
\rho_f(\rho(g')) &= \sum_{g \in G} f(g)\rho(g)\rho(g') && \text{by definition of } \rho_f \\
&= \sum_{g \in G} f(g)\rho(gg') && \text{since } \rho \text{ is a homomorphism} \\
&= \sum_{g \in G} f(g)\rho(g'(g')^{-1}gg') && \text{multiplying by } g'(g')^{-1} = e) \\
&= \sum_{g \in G} f(g)\rho(g')\rho((g')^{-1}gg') && \text{since } \rho \text{ is a homomorphism} \\
&= \rho(g') \sum_{g \in G} f(g)\rho((g')^{-1}gg') && \text{since } \rho(g') \text{ does not depend on } g \\
&= \rho(g') \sum_{g \in G} f(g'((g')^{-1}gg')(g')^{-1})\rho((g')^{-1}gg') \\
&= \rho(g') \sum_{g \in G} f((g')^{-1}gg')\rho((g')^{-1}gg') && \text{since } f \text{ is a class function} \\
&= \rho(g')\rho_f && \text{by definition of } \rho_f
\end{aligned}$$

This show that ρ_f satisfies the requirements of Schur's Lemma, and since ρ is irreducible we have that ρ_f is a scalar multiple of the identity.

Since $\rho_f = \lambda I$ we have that $\mathrm{tr}(\rho_f) = \lambda d$ where d is the degree of ρ. By definition we have that $\mathrm{tr}(\rho(g)) = \chi(g)$, hence

$$\begin{aligned}
\mathrm{tr}(\rho_f) &= \mathrm{tr}\left(\sum_{g \in G} f(g)\rho(g)\right) \\
&= \sum_{g \in G} f(g)\chi_\rho(g) && \text{by definition of } \chi_\rho \\
&= |G| \langle f, \overline{\chi} \rangle && \text{by definition of inner product}
\end{aligned}$$

Since ρ is irreducible by theorem 5 we have that so is $\overline{\rho}$ and hence $\overline{\chi}$ is an irreducible character.
This means that this inner product is zero, and hence $\lambda = 0$.
Hence for any irreducible representation, $\rho_f = 0$. □

Notice that for abelian groups the set of class functions on G, denoted $\mathrm{Cl}(G)$ 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 $G \to \mathbb{C}$, 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**].

We will formalize this important result as a theorem for future reference:

Theorem 7. *If G is a finite group, then a basis can be chosen such that the matrix $M_\rho(g)$ is unitary. The set of these coefficients forms an orthogonal basis for $\mathbb{C}^G$, and the set $\{\sqrt{\dim(\rho)}(\rho, i, j)\}$ where (ρ, i, j) is the i, jth coefficient of the matrix $M_\rho(g)$ is an orthonormal basis for $\mathbb{C}^G$.*

2.5 The Quantum Fourier Transform

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 Section 2.2, 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 $\rho(g)(|i\rangle) \in \text{span}\{|i\rangle\}$.

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

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

using the basis of irreducible characters of G, which is an orthonormal basis for $\mathbb{C}^G$ by theorem 6.

For general non-abelian groups we recall from that the set of irreducible characters is not a basis for $\mathbb{C}^G$, but invoking theorem 7 we can use the set of scaled matrix coefficients as a basis, giving the *general Quantum Fourier Transform*:

$$\mathcal{F}_G(|g\rangle) = \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \hat{G}} \sqrt{\dim(\sigma)} \sum_{i,j=1}^{\dim(\sigma)} \sigma(g)_{i,j} \, |\sigma, i, j\rangle \tag{2}$$

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

Notice that for the case of abelian groups the general QFT is equivalent to that of the ablian 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.

Referring back to ection 2.2] we recall that any transformation we apply must be unitary. Fortunately for us, QFT is a unitary transform:

Theorem 8. *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 tranformation 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. □

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

Example 1.
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 $|i\rangle + |j\rangle = |i + j \mod 2\rangle$. 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

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

with characters

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

and

$$\chi_1(|i\rangle) = \left|(-1)^i\right\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} |i\rangle .$$

Given the standard basis for $\mathbb{C}^2$ given by $|0\rangle, |1\rangle$, we can apply the fourier transform as follows:

Recall that the general quantum fourier transform is given by

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

We apply this to our basis vectors:

$$\begin{aligned} \mathcal{F}_G(|0\rangle) &= \frac{1}{\sqrt{2}} \sum_{\sigma \in \hat{\mathbb{Z}}_2} \sqrt{\dim(\sigma)} \sum_{i,j=1}^{\dim(\sigma)} \sigma(|0\rangle)_{i,j} |\sigma, i, j\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{\sigma \in \hat{\mathbb{Z}}_2} \sqrt{2} \sum_{i,j=1}^{2} \sigma(|0\rangle) |\sigma, i, j\rangle \\ &= \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \end{aligned}$$

and

$$\begin{aligned} \mathcal{F}_G(|1\rangle) &= \frac{1}{\sqrt{2}} \sum_{\sigma \in \hat{\mathbb{Z}}_2} \sqrt{\dim(\sigma)} \sum_{i,j=1}^{\dim(\sigma)} \sigma(|1\rangle)_{i,j} |\sigma, i, j\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{\sigma \in \hat{\mathbb{Z}}_2} \sqrt{2} \sum_{i,j=1}^{2} \sigma(|1\rangle)_{i,j} |\sigma, i, j\rangle \\ &= \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \end{aligned}$$

3 The Hidden Subgroup Problem

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 23 (Separating Function)**.**
We say that a function $f : G \to X$ 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

$$f(g_1) = f(g_2) \iff g_1 H = g_2 H.$$

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

> **Problem 1** (Hidden Subgroup Problem)**.**
> Given a group G, a finite set X and a function $f : G \to X$ 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 Section 4

3.1 The Abelian Hidden Subgroup Problem

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.

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

> **Problem 2** (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 9. *the set $H = \{(xr, x) \mid x \in \mathbb{Z}_{p-1}\}$ is a subgroup of $g = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$.*

Proof. H is trivially a non-empty subset of G, so it remains only to check that H is a group.

Let $(sr, s), (tr, t) \in H$.
Notice that $(tr, t)^{-1} = (-tr, -t)$.
This is clearly of the form (xr, x) and hence is an element of H, hence H contains inverses for each element.

Notice also that $(tr, t) \cdot (sr, s) = (tr + sr, t + s) = ((t + s)r, ((t + s))$ which is of the form (xr, x) for $x = (t + s)$, hence H is closed.

Therefore H is a subgroup of G by the 2-step subgroup test, as wanted. □

Theorem 10. *$f(x, y) = g^x g^{-ry}$ separates cosets of H.*

In order to show this, we first prove a lemma:

Lemma 3.1. *$f(x, y) = 1 \iff (x, y) \in H$.*

Proof.

$\Longrightarrow$

Suppose $f(x,y)=1$.

$$\begin{aligned} & f(x,y)=1 && \\ \iff & g^{x-ry}=1 && \text{by definition of } f(x,y) \\ \iff & x-ry=0 && \text{in } \mathbb{Z}_p \\ \iff & x=ry && \\ \iff & (x,y)=(xr,x) && \end{aligned}$$

Hence $(x,y)\in H$.

$\Longleftarrow$

Suppose $(x,y)\in H$.
Then $(x,y)=(ra,a)$ for some $a\in G$.

$$\begin{aligned} g^{x-ry} &= g^{ra-ra} && \text{by definition of } f(x,y) \\ &= g^0 && \text{in } \mathbb{Z}_p \\ &= 1 && \end{aligned}$$

Hence $f(x,y)=1$.

Therefore $f(x,y)=1 \iff (x,y)\in H$, as wanted. □

We can now prove theorem 10.

Proof.

$\Longrightarrow$

Suppose $f(a)=f(b)$, where $a=(a_1,a_2), b=(b_1,b_2)\in G$.
Then:

$$\begin{aligned} f(a) &= f(b) && \\ g^{a_1-ra_2} &= g^{b_1-rb_2} && \text{by definition of } f \\ g^{a_1-ra_2-(b_1-rb_2)} &= 1 && \\ g^{(a_1-b_1)-r(a_2-b_2)} &= 1 && \\ f(a-b) &= 1 && \text{by definition of } f \end{aligned}$$

Hence $a-b\in H$ by lemma 3.1.
Since $a-b\in H$, $a+H=b+H$.

$\Longleftarrow$

Suppose $a+H=b+H$.
Then $a-b\in H$ and by lemma $f(a-b)=1$.

$$\begin{aligned} f(a-b) &= 1 && \\ g^{(a_1-b_1)-r(a_2-b_2)} &= 1 && \text{by definition of } f \\ g^{a_1-ra_2-(b_1-rb_2)} &= 1 && \\ g^{a_1-ra_2} &= g^{b_1-rb_2} && \\ f(a) &= f(b) && \text{by definition of } f \end{aligned}$$

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

Hence f separates cosets of H, and we can see that the discrete logarithm problem is an instance of the hidden subgroup problem. The discrete logarithm problem is a key problem used in many important public-key cryptographic systems, for example El-Gamal and the Diffie-Hellman key exchange. We can also generalize other problems, such as the period-finding problem and the order finding problem. These problems are the foundation of many modern cryptographic systems, and as a generalization of these, solving the HSP efficiently allows us to solve any of these problems efficiently.

3.2 Algorithms for Solving The Hidden Subgroup Problem

With an understanding of the HSP we can now begin to discuss how we might solve this problem using quantum computing.

3.3 The 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 $f : G \to X$. 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 ith 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 left of the tensor product, and the second register is represented by $|0\rangle$ on the right side.

Step 2: Evaluate f in the second register, producing the state

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

Step 3: Now measure the second register using the measurement system $\{M_x = |x\rangle \langle x| \mid x \in X\}$ given by orthogonal projection onto the span of orthonormal basis vectors of $\mathcal{H}$. This yields the outcome x with probability p_x. We determine p_x as follows:

$$\begin{aligned} p_x &= \left\| I \otimes M_x \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \right) \right\|^2 \\ &= \left\| \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes M_x |f(g)\rangle \right\|^2 && \text{distributing the tensor products} \\ &= \left\| \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |x\rangle \langle x| f(g)\rangle \right\|^2 && \text{by definition of } M_x \end{aligned}$$

Notice that since $\mathcal{H}$ is spanned by elements of X, we have that an orthonormal basis for $\mathcal{H}$ is given by elements of X, which can be written as $f(g)$ for some $g \in G$ by definition of X. This

gives that

$$\begin{aligned} p_x &= \left\| \frac{1}{\sqrt{|G|}} \sum_{g \in G, f(g)=x} |g\rangle \otimes |x\rangle \right\|^2 \\ &= \frac{|H|}{|G|} \end{aligned}$$

Of particular interest here is that p_x is independent of x.

If we suppose that x has occurred, then we are left with the state

$$\begin{aligned} |\phi\rangle &= \frac{1}{\sqrt{p_x}} I \otimes M_x \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \right) \\ &= \frac{\sqrt{|G|}}{\sqrt{|H|}} \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes M_x |f(g)\rangle && \text{distributing the tensor product} \\ &= \frac{1}{\sqrt{|H|}} \sum_{g \in G} |g\rangle \otimes |x\rangle \langle x| |f(g)\rangle && \text{by definition of } M_x \\ &= \frac{1}{\sqrt{|H|}} \sum_{g \in G, f(g)=x} |g\rangle \otimes |x\rangle \end{aligned}$$

This is the set of all elements of G that map to the value x. Since f is a hiding function, this means that we have recovered a coset cH of H. We make this cleared by writing

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

This state is a uniform superposition of elements of cH, and since $f(ch) = x$ for all $h \in H$ we can abbreviate this:

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

Step 4: The last step in this process is left open-ended; there are numerous ways to continue, but the important part of the coset sampling method is to attain the coset state. From here, various different types of measurements can be applied to deduce information about the coset. Some examples include deducing an element of H, or a multiple of the order of H.

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

Example 2.
Let $G = \mathbb{Z}_6, H = \{0, 3\}$. We can find the cosets of H are as follows:

$$\begin{aligned} H &= \{0, 3\} \\ 1 + H &= \{1, 4\} \\ 2 + H &= \{2, 5\} \end{aligned}$$

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

$$\begin{aligned} f(H) &= 0 \\ f(1 + H) &= 1 \\ f(2 + H) &= 2 \end{aligned}$$

From these definitions we can determine the values mentioned in subsection section 3.3, the abstract description of this method. We first examine f and notice that $X = \{0, 1, 2\}$. We now

search for $\mathcal{G}$ and $\mathcal{H}$. Recall that these are Hilbert spaces spanned by X and G respectively. Since $X = \{0, 1, 2\}$ does not represent an orthonormal basis if we were to take this directly to a familiar vector space such as $\mathbb{R}$, we can either re-define our inner product on this space to generate a reasonable Hilbert space, or more conveniently we can take $\mathcal{H} = \text{span}\{X\} = \text{span}\{|0\rangle, |1\rangle, |2\rangle\}$. Similarly for $\mathcal{G}$ we can take $\mathcal{G} = \text{span}\{G\} = \text{span}\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle\}$. In essence, given X and G, we take the ith element of each to the basis vector e_i in $\mathcal{H}$ and $\mathcal{G}$ respectively.

We proceed to solve this using the coset sampling method. As mentioned, step 1 is to create two registers (recall that both registers are represented in a single state, written as a tensor product of the registers). In this example, the first state is given by

$$|\psi_1\rangle = \frac{1}{\sqrt{6}} \sum_{g \in \mathbb{Z}_6} |g\rangle \otimes |0\rangle$$

Next, we evaluate f on the first register and store it in the second.

$$|\psi_2\rangle = \frac{1}{\sqrt{6}} \sum_{g \in \mathbb{Z}_6} |g\rangle \otimes |f(g)\rangle$$

Measuring with respect to the basis of elements of G using $M_x = |x\rangle \langle x|$ we obtain outcome x, giving

$$|\phi\rangle = \frac{1}{\sqrt{2}} \sum_{g \in \mathbb{Z}_6, f(g) = x} |g\rangle \otimes |x\rangle .$$

For the sake of this example suppose that $x = 1$. Then we can write $|\psi_2\rangle$ explicitly as the superposition

$$|\psi_2\rangle = \frac{1}{\sqrt{6}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle + |3\rangle \otimes |0\rangle + |4\rangle \otimes |1\rangle + |5\rangle \otimes |2\rangle \right)$$

We then apply our measurement. Recall that $p_x = \frac{|H|}{|G|}$, and so we obtain

$$\begin{aligned}
|\phi\rangle &= \frac{1}{\sqrt{p_x}} I \otimes M_x \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \right) \\
&= \frac{\sqrt{6}}{\sqrt{|2|}} \frac{1}{\sqrt{|6|}} \sum_{g \in \mathbb{Z}_6} |g\rangle \otimes M_x |f(g)\rangle && \text{distributing tensor product} \\
&= \frac{1}{\sqrt{2}} \sum_{g \in \mathbb{Z}_6} |g\rangle \otimes |x\rangle \langle x| |f(g)\rangle && \text{by definition of } M_x \\
&= \frac{1}{\sqrt{2}} (\\
&\quad |0\rangle \otimes |1\rangle \langle 1| |0\rangle + \\
&\quad |1\rangle \otimes |1\rangle \langle 1| |1\rangle + \\
&\quad |2\rangle \otimes |1\rangle \langle 1| |2\rangle + \\
&\quad |3\rangle \otimes |1\rangle \langle 1| |0\rangle + \\
&\quad |4\rangle \otimes |1\rangle \langle 1| |1\rangle + \\
&\quad |5\rangle \otimes |1\rangle \langle 1| |2\rangle) && \text{expanding the sum}
\end{aligned}$$

Recall that $\langle x| |y\rangle = \langle x, y\rangle = 0$ for $x \neq y$ since these are orthogonal basis vectors. This leaves

$$|\phi\rangle = \frac{1}{\sqrt{2}} |1\rangle + \frac{1}{\sqrt{2}} |4\rangle$$

Which is clearly a uniform superposition of a coset of H, as expected.

4 Non-Abelian HSP

4.1 Dihedral Groups

For the sake of this report, we define $D_{2n} = \langle r, s \mid r^n = s^2 = rsrs = e \rangle$.

Theorem 11. *D_{2p} has $p+3$ subgroups.*

> **Example 3.**
> 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 $\langle e \rangle$.
>
> Hence we have found H.

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

The proof of this is provided in [**perepechaenko**].

Theorem 13. *If $G = D_{2n}$ and $H \leqslant G$ be a subgroup hidden by the function $f : G \to X$. Then $f|_{C_n} : C_n \to X$ 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 abelian QFT in order to gain information about H and f.