The Hidden Subgroup Problem

River McCubbin With Supervisor Camelia Karimian-Pour

August 16, 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.

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* $\phi : V \to W$ 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 Algebra: Operators

Definition (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 $a, b \in \mathbb{F}$.

Definition (Adjoint Operator)

Given an operator $\phi : \mathcal{H} \to \mathcal{H}$ 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^*.

Linear Algebra: Operators

Definition (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 $a, b \in \mathbb{F}$.

Definition (Adjoint Operator)

Given an operator $\phi : \mathcal{H} \to \mathcal{H}$ 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 $U : \mathcal{H} \to \mathcal{H}$ 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 $aa^{-1} = a^{-1}a = e$.

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

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!

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

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

[1] the $\cdot$ 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 $H \leqslant G$ if it may be equal, and $H < G$ if $H \neq G$.

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

Definition (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 $Ha = \{h \cdot a \mid h \in H\}$.

Group Theory: Generating Groups

Definition (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.

Group Theory: Generating Groups

Definition (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.

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.

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 $G = \{e, r, r^2 \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\} = \langle r, s \mid r^n = s^2 = srsr = e \rangle$.

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 write D_{2n} for this group.

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 write D_{2n} for this group.
D_{2n} represents the symmetries of an n-gon.

Group Theory: Morphisms on Groups

Definition (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 $a, b \in G$.

Group Theory: Morphisms on Groups

Definition (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 (Isomorphism)

A function $f : G \to K$ 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.

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.

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 $w \in W$.

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 $v \otimes w$.

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.

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.

Quantum Computing: Bra-Ket Notation

- column vectors: $|\psi\rangle$ (read "ket psi").

Quantum Computing: Bra-Ket Notation

- column vectors: $|\psi\rangle$ (read "ket psi").
- row vectors: $\langle\psi|$ (read "bra psi"), map $\langle\psi| : \mathcal{H} \to \mathbb{C}$, the adjoint of $|\psi\rangle$.

Quantum Computing: Bra-Ket Notation

- column vectors: $|\psi\rangle$ (read "ket psi").
- row vectors: $\langle\psi|$ (read "bra psi"), map $\langle\psi| : \mathcal{H} \to \mathbb{C}$, the adjoint of $|\psi\rangle$.

Why?

Quantum Computing: Bra-Ket Notation

- column vectors: $|\psi\rangle$ (read "ket psi").
- row vectors: $\langle\psi|$ (read "bra psi"), map $\langle\psi| : \mathcal{H} \to \mathbb{C}$, the adjoint of $|\psi\rangle$.

Why?

$$\langle\psi|\,|\phi\rangle = \langle\psi\,|\,\phi\rangle = \langle\psi, \phi\rangle$$

Quantum Computing: More Notation

An abbreviate: $|ab\rangle := |a\rangle \otimes |b\rangle$.

Quantum Computing: More Notation

An abbreviate: $|ab\rangle := |a\rangle \otimes |b\rangle$.Simplify:

Quantum Computing: More Notation

An abbreviate: $|ab\rangle := |a\rangle \otimes |b\rangle$.Simplify:

- first basis vector is $|0\rangle$.

Quantum Computing: More Notation

An abbreviate: $|ab\rangle := |a\rangle \otimes |b\rangle$.Simplify:

- first basis vector is $|0\rangle$.
- second basis vector is $|1\rangle$.

Quantum Computing: More Notation

An abbreviate: $|ab\rangle := |a\rangle \otimes |b\rangle$.Simplify:

- first basis vector is $|0\rangle$.
- second basis vector is $|1\rangle$.
- third basis vector is $|2\rangle$.

Quantum Computing: More Notation

An abbreviate: $|ab\rangle := |a\rangle \otimes |b\rangle$.Simplify:

- first basis vector is $|0\rangle$.
- second basis vector is $|1\rangle$.
- third basis vector is $|2\rangle$.
- nth basis vector is $|n-1\rangle$.

Quantum Computing: Larger Spaces

Theorem

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

Quantum Computing: Larger Spaces

Theorem

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

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.

Quantum Computing: Larger Spaces Example I

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

Quantum Computing: Larger Spaces Example I

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 $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$.

Quantum Computing: Larger Spaces Example I

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:

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

Quantum Computing: Larger Spaces Example II

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

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

Quantum Computing: Larger Spaces Example II

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

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

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
$|\psi\rangle = a\,|0\rangle + b\,|1\rangle + \cdots + c\,|2^n - 1\rangle$.

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

How do we perform an operation on our data (vectors)?

Quantum Computing: How to Compute

How do we perform an operation on our data (vectors)?Recall: We only work with unit vectors.

Quantum Computing: How to Compute

How do we perform an operation on our data (vectors)?Recall: We only work with unit vectors.Hence: operations take and output unit vectors.

Quantum Computing: How to Compute

How do we perform an operation on our data (vectors)?Recall: We only work with unit vectors.Hence: operations take and output unit vectors.These operators are unitary operators, mentioned before.

Quantum Computing: How to Compute

How do we perform an operation on our data (vectors)?Recall: We only work with unit vectors.Hence: operations take and output unit vectors.These operators are unitary operators, mentioned before.Unitary operators can be used as logic gates, ex. AND, NOT, OR etc.

Quantum Computing: Quantum NOT Gate Example

Quantum NOT gate is given by

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

Quantum Computing: Quantum NOT Gate Example

Quantum NOT gate is given by

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

Verifying:

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

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

Quantum Computing: Quantum NOT Gate Example

Quantum NOT gate is given by

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

Verifying:

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

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

Notice that this is a 2D rotation matrix on the x axis.

Quantum Computing: Quantum NOT Gate Example

Quantum NOT gate is given by

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

Verifying:

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

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

Notice that this is a 2D rotation matrix on the x axis.
There are corresponding gates for other axes and in higher dimension.

Quantum Computing: Limitations

No universal gate, classical examples are NAND, NOR.

Quantum Computing: Limitations

No universal gate, classical examples are NAND, NOR.
This means specialized circuits for quantum computing.

Quantum Computing: Measurement

How do we regain information after processing?

Quantum Computing: Measurement

How do we regain information after processing?
Problem:

Quantum Computing: Measurement

How do we regain information after processing?
Problem: Cannot observe directly.

Quantum Computing: Measurement

How do we regain information after processing?
Problem: Cannot observe directly.
Solution:

Quantum Computing: Measurement

How do we regain information after processing?
Problem: Cannot observe directly.
Solution:
Require a separable state.

Quantum Computing: Measurement

How do we regain information after processing?
Problem: Cannot observe directly.
Solution:
Require a separable state.
"Collapse" to a basis vector.

Quantum Computing: Measurement Operators

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

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

and the state after measurement is given by

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

Quantum Computing: Measurement Example

Example: projection matrices on $\mathbb{C}^2$ are measurement operators.

Quantum Computing: Measurement Example

Example: projection matrices on $\mathbb{C}^2$ are measurement operators.These matrices are given by

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

and

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

Verify:

$$P_x + P_y = I$$

is satisfied.

Quantum Computing: Measurement Example

Example: projection matrices on $\mathbb{C}^2$ are measurement operators.These matrices are given by

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

and

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

Verify:

$$P_x + P_y = I$$

is satisfied.
Projection matrices are unitary.

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

Definition (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, 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 $\rho : G \to GL(V)$, we define the *character* χ_ρ[2] of ρ as the map $\chi_\rho : G \to \mathbb{C}$ given by $\chi_\rho(g) = \mathrm{tr}\,(\rho(g))$.

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.

[2] often 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

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

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 $\rho_1 : G \to GL(V), \rho_2 : G \to GL(W)$ of a group G are called *isomorphic*[3] if there exists an isomorphism $\phi : V \to W$ such that $\phi(\rho_1(g)(v)) = \rho_2(g)(\phi(v)), \forall v \in V, \forall g \in G$. We write $\rho_1 \cong \rho_2$.

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

[3] the 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 $\rho_1 : G \to GL(V)$ and $\rho_2 : G \to GL(W)$. Let $f : GL(V) \to GL(W)$ 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 $h : V \to W$ 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 $h_0 = \frac{\mathrm{tr}(h)}{\dim(V)} I$.*

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 26 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 [Ser77]. □

Representation Theory: Conjugate Representation

Definition (Conjugate Representation)

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

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

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

Representation Theory: Conjugate Characters

Theorem

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

Theorem

The conjugate of an irreducible representation is irreducible.

Representation Theory: Conjugate Representation Proof

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

$$\begin{aligned}
\langle \chi_{\overline{\rho}}, \chi_{\overline{\rho}} \rangle &= \langle \overline{\chi_\rho}, \overline{\chi_\rho} \rangle && \text{by 31} \\
&= \langle \chi_\rho, \chi_\rho \rangle && \text{by definition of inner product} \\
&= 1 && \text{by 26 since } \rho \text{ is irreducible}
\end{aligned}$$

Hence $\overline{\rho}$ is irreducible by 26. □

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

Representation Theory: Class Functions

Definition (Class Function)

A function $f : G \to V$ 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 $\hat{G} = \{\chi_0 \ldots, \chi_{N-1}\}$ of all irreducible characters of G forms an orthonormal basis for the space of class function on G.

As shown in 29, 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.

Representation Theory: An Orthonormal Basis Proof I

Let $g' \in G$ be arbitrary.
Then:

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

by definition of ρ_f

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

since ρ is a homomorphism

$$= \sum_{g \in G} f(g)\rho(g'(g')^{-1}gg')$$

multiplying by $g'(g')^{-1} = e$)

Representation Theory: An Orthonormal Basis Proof II

$$= \sum_{g \in G} f(g)\rho(g')\rho((g')^{-1}gg')$$

since ρ is a homomorphism

$$= \rho(g') \sum_{g \in G} f(g)\rho((g')^{-1}gg')$$

since $\rho(g')$ does not depend on g

$$= \rho(g') \sum_{g \in G} f(g'((g')^{-1}gg')(g')^{-1})\rho((g')^{-1}gg')$$

$$= \rho(g') \sum_{g \in G} f((g')^{-1}gg')\rho((g')^{-1}gg')$$

since f is a class function

$$= \rho(g')\rho_f$$

by definition of ρ_f

Representation Theory: An Orthonormal Basis Proof III

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

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

Since ρ is irreducible by 32 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, $\rho_f = 0$, as wanted.

Representation Theory: Abelian vs. Non-Abelian Bases

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 [Per21] and [Ser77].

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 25, 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

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

using the basis of irreducible characters of G, which is an orthonormal basis for $\mathbb{C}^G$ by 34.

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 35 we can use the set of scaled matrix coefficients as a basis, giving the *general Quantum Fourier Transform*:

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

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 $|\sigma, i, j\rangle(g) = \langle i| \sigma(g) |j\rangle$.

QFT: Equivalent Transforms

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.

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 [Per21], 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. □

QFT: Example I

This definition can appear intimidating, and so we now examine an example of applying the quantum fourier transform, based on [Had20]. 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

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

QFT: Example II

The characters of these representations are given by

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

and

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

respectively. 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

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

QFT: Example III

We apply this to our basis vectors. For $|0\rangle$ we get

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

QFT: Example IV

And for $|1\rangle$ we get

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

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 $f : G \to X$ 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

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

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 $f : G \to X$ 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 64

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: DLP I

An example of the Hidden Subgroup Problem over abelian groups is the Discrete Logarithm Problem (DLP). 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.

Abelian HSP: DLP II

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.

Abelian HSP: DLP: H is a Subgroup

We now show that H is in fact a subgroup, and that f separates cosets of H.

Theorem

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

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.

Abelian HSP: DLP: f Separates Cosets of H

Theorem

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

Abelian HSP: DLP: Lemma I

Lemma

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

$\Longrightarrow$

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 $(x, y) \in H$.

Abelian HSP: DLP Lemma II

$$\Longleftarrow$$

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.

Abelian HSP: DLP: f Separates Cosets of H Proof I

$$\Longrightarrow$$

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 42.
Since $a - b \in H$, $a + H = b + H$.

Abelian HSP: DLP: f Separates Cosets of H Proof II

$$\Longleftarrow$$

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.

Abelian HSP: DLP is an Instance of HSP

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.

Algorithms for HSP: Coset Sampling Method Setup

The most common method for solving the HSP is the *Coset Sampling Method*.
The coset sampling method is described in [Per21] 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.

Algorithms for HSP: Coset Sampling Method 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.

Algorithms for HSP: Coset Sampling Method Step 2

Evaluate f in the second register, producing the state

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

Algorithms for HSP: Coset Sampling Method Step 3 I

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:

$$p_x = \left\| I \otimes M_x \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \right) \right\|^2$$

$$= \left\| \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes M_x |f(g)\rangle \right\|^2$$

distributing the tensor products

$$= \left\| \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |x\rangle\langle x| |f(g)\rangle \right\|^2$$

by definition of M_x

Algorithms for HSP: Coset Sampling Method Step 3 II

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.

Algorithms for HSP: Coset Sampling Method Step 3 III

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

$$|\phi\rangle = \frac{1}{\sqrt{p_x}} I \otimes M_x \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \right)$$

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

distributing the tensor product

$$= \frac{1}{\sqrt{|H|}} \sum_{g \in G} |g\rangle \otimes |x\rangle \langle x| |f(g)\rangle$$

by definition of M_x

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

Algorithms for HSP: Coset Sampling Method Step 3 IV

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:

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

Algorithms for HSP: Coset Sampling Method 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.

Coset Sampling Method: Example I

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

$$H = \{0, 3\}$$
$$1 + H = \{1, 4\}$$
$$2 + H = \{2, 5\}$$

Coset Sampling Method: Example II

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

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

Coset Sampling Method: Example III

From these definitions we can determine the values mentioned in subsection **??**, 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.

Coset Sampling Method: Example IV

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

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

Coset Sampling Method: Example V

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

$$
\begin{aligned}
|\psi_2\rangle = \frac{1}{\sqrt{6}}(& \\
& |0\rangle \otimes |0\rangle + \\
& |1\rangle \otimes |1\rangle + \\
& |2\rangle \otimes |2\rangle + \\
& |3\rangle \otimes |0\rangle + \\
& |4\rangle \otimes |1\rangle + \\
& |5\rangle \otimes |2\rangle \\
&)
\end{aligned}
$$

Coset Sampling Method: Example VI

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

$$|\phi\rangle = \frac{1}{\sqrt{p_x}} I \otimes M_x \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \right)$$

$$= \frac{\sqrt{6}}{\sqrt{|2|}} \frac{1}{\sqrt{|6|}} \sum_{g \in \mathbb{Z}_6} |g\rangle \otimes M_x |f(g)\rangle$$

distributing tensor product

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

by definition of M_x

Coset Sampling Method: Example VII

$$
\begin{aligned}
& \frac{1}{\sqrt{2}}(\\
= \quad & |0\rangle \otimes |1\rangle \langle 1| \, |0\rangle + \\
& |1\rangle \otimes |1\rangle \langle 1| \, |1\rangle + \\
& |2\rangle \otimes |1\rangle \langle 1| \, |2\rangle + \\
& |3\rangle \otimes |1\rangle \langle 1| \, |0\rangle + \\
& |4\rangle \otimes |1\rangle \langle 1| \, |1\rangle + \\
& |5\rangle \otimes |1\rangle \langle 1| \, |2\rangle)
\end{aligned}
\qquad \text{expanding the sum}
$$

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.

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.

Non-Abelian HSP: A Classical Attack

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.

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 Quantum Method for Solving HSP over D_{2n}

Theorem

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 $H \cap C_n$.

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

Conclusion

1. Abelian HSP is solvable
2. Non-Abelian HSP over dihedral can be reduced to abelian

Conclusion II: Future Study

1. Can other non-abelian groups be reduced to abelian?
2. How can we most efficiently extract information in step 4 of the coset sampling method?
3. Can we develop algorithms more efficient than QFT?

The End!

Thank you!

[Gre93] George D. Greenwade. "The Comprehensive Tex Archive Network (CTAN)". In: *TUGBoat* 14.3 (1993), pp. 342–351.

[Had20] Charles Hadfield. "Representation theory behind the quantum Fourier transform". In: (2020). URL: https://math.berkeley.edu/~hadfield/post/fourier/.

[Lom04] Chris Lomont. "The Hidden Subgroup Problem - Review and Open Problems". In: (2004).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computing and Quantum Information*. Cambridge University Press, 2010.

[Per21] Maria Perepechaenko. "Hidden Subgroup Problem - About some classical and quantum algorithms.". In: (2021).

[Ser77] J. P. Serre. *Linear Representations of Finite Groups*. Springer-Verlag, 1977.

[Ste12] Benjamin Steinberg. *Representation Theory of Finite Groups*. springer, 2012.