The Hidden Subgroup Problem

River McCubbin With Supervisor Camelia Karimian-Pour

August 17, 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

Motivation

Public key cryptography.

- Diffie-Hellman
- El-Gamal

Motivation

Public key cryptography.

- Diffie-Hellman
- El-Gamal

The cryptographic problems:

- Discrete Logarith Problem
- Period-Finding problem
- Order-Finding problem

Linear Algebra Overview

- Hilbert Space
- Linear, Adjoint, Unitary Operators

Group Theory Overview

1. Finite Groups, Subgroups, Cosets
2. Generators
3. Cyclic, Dihedral Groups
4. Homomorphisms, Isomorphisms

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: 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

Abbreviation: $|ab\rangle := |a\rangle \otimes |b\rangle$.

Quantum Computing: More Notation

Abbreviation: $|ab\rangle := |a\rangle \otimes |b\rangle$.
Simplified: nth basis vector is $|n-1\rangle$.

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 a linear combination of basis vectors.

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 a linear combination of basis vectors.

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: 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 represent possible outcomes. If the state of the system before measurement is ψ, then the probability result m occurs is

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

and the state after measurement is

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

These are typically orthogonal projection operators.

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.

Takes group elements of G to functions acting on V.

Representation Theory: Characters

Definition (Character)

Given a group G with a representation $\rho : G \to GL(V)$, we define the *character* χ_ρ[1] of ρ as the map $\chi_\rho : G \to \mathbb{C}$ given by $\chi_\rho(g) = \mathrm{tr}\,(\rho(g))$.

Carries information about a representation more concisely.

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

Representation Theory: Inner Product of Functions on G

Definition (Inner Product of Functions on G)

Given $f, h : G \to \mathbb{C}$ are functions on G we define their inner product to be

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

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*.

Theorem

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

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 $\mathbb{C}^G$, the space of class function on G.

For abelian groups this is all functions.

Representation Theory: Abelian vs. Non-Abelian Bases

Theorem

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 $\mathbb{C}^G$.

QFT: Abelian QFT

The abelian QFT is given by

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

It is a change to the basis of irreducible characters of G.

QFT: general QFT

The general QFT is given by

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

It is a change to the basis of matrix coefficients of irreducible representations of G.
Here $|\sigma, i, j\rangle : GL(V) \to \mathbb{Z}$ takes a group element g to its matrix coefficient at i, j under σ, i.e. $|\sigma, i, j\rangle(g) = \langle i| \sigma(g) |j\rangle$.

HSP: Separating Function

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

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.

Solved classically by evaluating $f(g)$ for every $g \in G$, but this method is incredibly inefficient.

Algorithms for HSP: Coset Sampling Method Setup

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: ψ_i denotes the ith state vector of our program.

Algorithms for HSP: Coset Sampling Method Step 1

Prepare two registers. The first register contains a uniform superposition of the elements of G. The second register is initialized to $|0\rangle$, and later will store states of $\mathcal{H}$.

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

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 on the first register and store evaluations in the second register, giving

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

Algorithms for HSP: Coset Sampling Method Step 3 I

Measure the second register using the measurement system $\{M_x = |x\rangle\langle x| \mid x \in X\}$ given by projection onto basis vectors of $\mathcal{H}$. This yields 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

Since $\mathcal{H}$ is spanned by X, an orthonormal basis for $\mathcal{H}$ is the elements of X, written as $f(g)$ for some $g \in G$ by definition. Hence

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

Notice that p_x is independent of x.

Algorithms for HSP: Coset Sampling Method Step 3 III

If x has occurred then we the state is

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

The set of elements of G that map to x under f.

Algorithms for HSP: Coset Sampling Method Step 3 IV

Since f is a hiding function, we have recovered a coset cH of H. We re-write our state as

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

This state is a uniform superposition 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 is open-ended; the goal 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.

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.