The hidden subgroup problem

Sumeet Shirgure
USC ID : 9330099198

Objectives

- Understanding the hidden subgroup problem (HSP)
  - Refresher on group theory
  - Statement of the problem and general solution approach for abelian HSPs
  - (Bare bones) introduction to representation theory of finite groups, and the corresponding Fourier transformation rules
- Reduction of a couple of well known problems to kinds of HSP
  - Discussion of reductions / current state

Group theory - axiomatic view

- Groups are abstract algebraic structures. A group is defined as a set G together with a group operation $(\cdot)$ that satisfies the axioms :
    - Closure - The result of an operation is again in G $a \cdot b \in G$
    - Associativity - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
    - Identities - $\exists e \in G : \forall a \in G a \cdot e = e \cdot a = a$
    - Inverses - $\exists ! a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$
    - If the group operation is commutative, the group is called abelian
        - $\forall a, b \in G, a \cdot b = b \cdot a$
        - Note that it's not always the case - e.g : the set of real valued n x n matrices under the usual matrix multiplication forms a (non-abelian) group.
- The size of the set $|G|$ is called the order of the group. We will be dealing only with finite groups.

Group theory - symmetry groups and subgroups

- Another way to look at groups is to look at the permutations of some n sized set X. Consider the set of all bijections $S_n \equiv \{f | f : X \to X\}$ $|S_n| = n!$
- It forms what is called the symmetric group of order n under composition.
- Groups let us model and study symmetry preserving operations :
    - E.g the set of all n permutations that leave some cyclic order unchanged forms a subset of S_n Note that it's the same as the set of remainders modulo n under addition - Z_n
- If some subset of the original group again forms a group under the same operation, it's called a subgroup.
- If we also allow reversal of the cyclic order, the resulting group is called the Dihedral group of order 2n, denoted D_n e.g permutations in D_3 map 012 to 012,120,201, 021,210,102 respectively

Group theory - generators

$$g, g^2, g^3, \ldots$$

- Given an arbitrary group G, consider any element g. Collect all powers of g. Since the group is finite, we must loop around at some point, implying every element g has what's called its *order*(g): smallest power r such that $g^r = e$
- The set$< g > \equiv \{e, g, g^2, \ldots, g^{r-1}\}$is a group *generated by* g.
  - E.g 2 generates {0,2,4} Z6, 3 generates {0,3} in Z6, 5 generates all of Z6
- Generalize this notion to the subgroup *generated* by elements $\{g_1, g_2, \ldots, g_k\}$
  - The subset of all group elements formed by repeated group operations within the set.
  - Any finite group G has a set of generators with sizemost log(|G|) (idea : repeated doubling)
  - E.g : D_n is generated by two operations $\{r, f\}; r^n = e = f^2, f \cdot r \cdot f = r^{-1}$

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, f \cdot r, f \cdot r^2, \ldots, f \cdot r^{n-1}\}$$

Group theory - cosets and Lagrange’s theorem

- For a group G and its subgroup K, the set $g \cdot K \equiv \{g \cdot k | k \in K\}$ is called a (left) coset of K in G.
  - Easier to understand with an example : $G = Z_{12}, K = \{0, 4, 8\}$ Then $1 + K = \{1, 5, 9\}, 2 + K = \{2, 6, 10\}, 3 + K = \{3, 7, 11\}$ are its cosets in G.
- Cosets partition G: the relation $(a, b) \iff a \cdot b^{-1} \in K$ is an equivalence relation on G, and the corresponding partitions are cosets
  - Hence, the [G : K] * |K| = |G|, or |K| divides |G|.
  - Corollary : order of any element in G divides |G| since <g> forms a subgroup of G
- We say that some function f on G “hides” K, or is “K periodic”, when

$$f(a) = f(b) \iff a \cdot K = b \cdot K$$

The function is constant on cosets and differs between them.

The hidden subgroup problem

Let G be a finitely generated group, and X be a finite set, and f : G --> X a function that hides a subgroup H of G (given by an oracle using O(log|G|+log|X|) bits as input to evaluate f(g)=x), “determine” the subgroup.

- Note - to determine the subgroup, we only need some generators for H. If some set A generates all of G, then some subset of A must generate H.
- Even if we have some generators, we also need their orders to do something useful.

Solving HSP for abelian groups.

There exists a polynomial time quantum algorithm for solving HSPs over abelian groups. We have already seen it as the period finding subroutine in Shor’s algorithm, where$G = Z_{2^n}$, and the hidden subgroup $H = < a >$ Where a is the element whose order we need to find.

To solve for the most general case of arbitrary finite abelian groups, we must first

- Look at the pretty neat characterization of abelian groups
- Look at some ideas from representation theory, as it will also help us in the non-abelian case, which don’t have an efficient algorithm

Group homomorphisms and isomorphisms

A structure preserving injection from a group (G,.) to (H,*) is called a homomorphism $\phi : G \rightarrow H | \phi(a \cdot b) = \phi(a) \star \phi(b)$

E.g - $\phi : Z_n \rightarrow U(1) | \phi(a) = e^{2\pi i a/n}$

Another example is the familiar determinant : $det : GL(V) \rightarrow V$

If the map is a bijection, the homomorphism is an isomorphism. Group isomorphism is the notion we use to say one group is the “same” as another.

Isomorphism carries over naturally to other discrete structures like graphs as well.

Direct product of groups

For groups $(G, \cdot), (H, *)$ the cartesian product $G \times H \equiv \{(g, h) | g \in G, h \in H\}$ forms a group element-wise operation : $(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 * h_2)$

This construction is called the external direct product of G and H.

$$G \times G = G^2$$

Fundamental theorem of finite abelian groups

Here are some facts about abelian groups:

- All cyclic groups <g> of order n are abelian and are isomorphic to Z_n given by the isomorphism : $\phi : Z_n \rightarrow < g > |\phi(x) = g^x$
- $Z_{mn} \cong Z_m \times Z_n \iff gcd(m, n) = 1$
    - Z_{15} is the same as the set of ordered tuples $\{(a, b)|a \in Z_3, b \in Z_5\}$
    - And also $Z_2 \times Z_2 \ncong Z_4$
- The fundamental theorem states that every abelian group has a factorization into cyclic groups of prime powers :
    - $Z_2 \times Z_2 \times Z_3$ and $Z_4 \times Z_3$ are the only abelian groups of order 12
    - There exists a generating set where each element has prime-power order

Representation theory (for finite abelian groups)

A representation ρ of a group G is a group homomorphism from G to the group of complex unitary matrices of some size n.

Quite a sophisticated theory. A lot of stuff is simplified for abelian groups.

A fundamental theorem from this domain is that every abelian group G has 1 dimensional representations, and there are exactly |G| distinct representations.

1D unitary matrices are just complex numbers on the unit circle.

E.g the three representations of Z_3 are

$$\rho_0(x) = 1, \rho_1(x) = e^{2\pi ix/3}, \rho_2(x) = e^{4\pi ix/3}$$

Representation theory (for finite abelian groups)

Each of the |G| distinct representations can be parametrized using the elements *in the group G itself.* We do this by mapping each generator g to an r'th root of 1 :

Let $G \cong Z_{p_1} \times Z_{p_2} \times \ldots \times Z_{p_k}$ be an arbitrary abelian group.

The k-tuples $g_1 = (1, 0, 0, \ldots), g_2 = (0, 1, 0, ..) \ldots$ form a k sized generating set for G. Any element $x \in G$ is a sum of the form $\sum_j x_j g_j$

We define the representation parametrized by h as :

$$\rho_h(x) = exp\left\{ 2\pi i \sum_j \frac{h_j x_j}{p_j} \right\}$$

Representation theory (for finite abelian groups)

E.g : For the group $Z_2 \times Z_2 = \{00, 01, 10, 11\}$, the four representations are :

$$\rho_{00} = \{1, 1, 1, 1\} \ \rho_{01} = \{1, -1, 1, -1\} \ \rho_{10} = \{1, 1, -1, -1\} \ \rho_{11} = \{1, -1, -1, 1\}$$

Some important properties of these representations are :

- Symmetry : $\rho_h(x) = \rho_x(h)$
- Orthogonality : $\sum_{h \in G} \rho_h(t) = \delta_{te} |G|$

Where e=(0,0,..) is the identity of group G

Representation theory - Fourier transform

Ultimately we want to study functions on groups $f : G \rightarrow X$ (the oracle kind.)

The set of functions on G $\{f|f : G \rightarrow \mathbb{C}\}$ form a complex vector space $\cong \mathbb{C}^{|G|}$

A convolution of two functions on G is defined as : $f * g(s) \equiv \sum_{t \in G} f(t)g(t^{-1}s)$

The Fourier transform of a function f is defined as the *Linear transform* :

$$\widehat{f}(\rho_h) \equiv \sqrt{\frac{d_\rho}{|G|}} \sum_{s \in G} \rho_h(s) f(s)$$

$$\widehat{f}(\rho_h)\widehat{g}(\rho_h) = \frac{1}{|G|} \sum_{s,t \in G} f(s)g(t)\rho_h(st) = \frac{1}{|G|} \sum_{v \in G} (f * g)(u)\rho_h(u) = \widehat{(f * g)}(\rho_h)$$

Representation theory - Fourier transform

E.g : For the group $Z_2 \times Z_2 = \{00, 01, 10, 11\}$, the function f can be written in a Fourier basis as follows :

$$\widehat{f}(\rho_{00}) = f(00) + f(01) + f(10) + f(11)$$
$$\widehat{f}(\rho_{01}) = f(00) - f(01) + f(10) - f(11)$$
$$\widehat{f}(\rho_{10}) = f(00) + f(01) - f(10) - f(11)$$
$$\widehat{f}(\rho_{11}) = f(00) - f(01) - f(10) + f(11)$$

Fourier inversion formula

The inversion formula reads : $f(s) \equiv \sqrt{\frac{d_\rho}{|G|}} \sum_{h \in G} Tr(\rho_h(s^{-1}) \widehat{f}(h))$

For abelian groups, it simplifies down to:

$$\widehat{f}(h) = \frac{1}{\sqrt{|G|}} \sum_{s \in G} \rho_h(s) f(s) \qquad f(s) = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \rho_h(s^{-1}) \widehat{f}(h)$$

In quantum algorithms, these transformations are represented as :

$$|\widehat{f}(h)\rangle = \frac{1}{\sqrt{|G|}} \sum_{s \in G} \rho_h(s) |f(s)\rangle \qquad |f(s)\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \rho_h(s^{-1}) |\widehat{f}(h)\rangle$$

Solution idea

- For a generic abelian group G, we must decompose it into its individual prime power cycles before sampling s. Note that this is at least as hard as factorization of |G|.
    - This is where Shor’s algorithm can be used! Turns out that the prime factorization of |G| contains enough information for us to be able to find the order of the generators of the subgroup that we are looking for.
- When |G| is not a power of 2, efficient quantum circuits do exist, and a good approximation scheme was given by Kitaev in his solution to the Abelian stabilizer problem, as a part of phase estimation procedure [6]
- Exact solution can be found in [7]

Fourier transform of periodic functions

Let $K < G$. Say K is generated by $K =< g_1, g_2, ..g_n >, n \leq k$

The group $< g_{n+1}, ..., g_k >$ is denoted by G/K

Consider the fourier transform a K periodic function : $\sqrt{|G|}|\widehat{f}(h)\rangle = \sum_{s \in G} \rho_h(s)|f(s)\rangle$

$$= \sum_{s_1 \in Z_{p_1}} ... \sum_{s_k \in Z_{p_k}} |f(s_1, s_2, ..., s_k)\rangle \rho_h(s)$$

$$= \sum_{s_{n+1} \in Z_{p_{n+1}}} ... \sum_{s_k \in Z_{p_k}} |f(s)\rangle \sum_{s_1 \in Z_{p_1}} ... \sum_{s_n \in Z_{p_n}} \rho_h(s)$$

The amplitude is $\sum_{s_1 \in Z_{p_1}} ... \sum_{s_n \in Z_{p_n}} exp\left\{2\pi i \sum_{j=1}^{k} \frac{h_j s_j}{p_j}\right\} = e^{2\pi i \phi_s} \sum_{s_1 \in Z_{p_1}} ... \sum_{s_n \in Z_{p_n}} exp\left\{2\pi i \sum_{j=1}^{n} \frac{h_j s_j}{p_j}\right\}$

Fourier transform of periodic functions

$$= e^{2\pi i\phi_s} \sum_{s_1\in Z_{p_1}} \dots \sum_{s_n\in Z_{p_n}} exp\left\{2\pi i \sum_{j=1}^{n} \frac{h_j s_j}{p_j}\right\}$$

$$= e^{2\pi i\phi_s} \sum_{s_1\in Z_{p_1}} \dots \sum_{s_n\in Z_{p_n}} \prod_{j=1}^{n} exp\left\{2\pi i \frac{h_j s_j}{p_j}\right\} = e^{2\pi i\phi_s} \prod_{j=1}^{n}\left\{\sum_{s_j\in Z_{p_j}} exp\left\{2\pi i \frac{h_j s_j}{p_j}\right\}\right\}$$

$$= e^{2\pi i\phi_s}|K|\delta_{h_1 0}\delta_{h_2 0}\dots\delta_{h_n 0} = e^{2\pi i\phi_s}|K|\delta_{h\in G/K}$$

I.e FT is non-zero only for representations in the factor group G/K

$$|\widehat{f}(h)\rangle = \frac{1}{\sqrt{|G|}} \sum_{s\in G/K} |f(s)\rangle \rho_h(s)|K|\delta_{h\in G/K}$$

Inverse Fourier transform of periodic functions

I.e FT is non-zero only for representations in the factor group G/K

$$|\widehat{f}(h)\rangle = \frac{1}{\sqrt{|G|}} \sum_{s \in G/K} |f(s)\rangle \rho_h(s) |K| \delta_{h \in G/K}$$

$$|f(s)\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} |\widehat{f}(h)\rangle \rho_h(s^{-1})$$

$$|f(s)\rangle = \frac{1}{\sqrt{|G/K|}} \sum_{h \in G/K} |\widehat{f}(h)\rangle \rho_h(s^{-1})$$

Some problems in HSP

All of the claimed “breaks” in cryptosystems like RSA/ECC arise from the ease of solving abelian HSPs, like factoring, or the discrete logarithm problem.

DLP can cast as an HSP: Given a group Z_p^* and a generator g, for some x in G, find the power r such that $g^r \equiv x (mod p)$. $Z_p^* = Z_p \setminus \{0\}$

We construct a new group $Z_p \times Z_p$ and an oracle $f(a,b) = g^a x^{-b}$

The kernel $ker\, f = \{(a,b) : f(a,b) = 1\}$ forms a subgroup of $Z_p \times Z_p$

f is periodic in that kernel, which is just the multiples of (r, 1)

Graph Isomorphism - a non abelian HSP

There also exist problems which can be cast as HSPs, but the group structure is non-abelian, making them difficult to solve. One such example is the Graph Isomorphism problem.

- Given two graphs $G_1(V_1, E_1), G_2(V_2, E_2)$, decide if they are isomorphic
- Interesting problem in its own right - $GI \in NP$ as the isomorphism $\phi : V_1 \to V_2, (u, v) \in E_1 \iff (\phi(u), \phi(v)) \in E_2$ is also a certificate.
- It is not known if GI is NP-complete - just like factoring.
- If the map goes from G to itself, the isomorphism is called an automorphism. GI can be reduced to finding automorphisms in a single graph.

Graph automorphism - a non abelian HSP

- Turns out GI is reducible to Graph automorphism
- The set of all automorphic permutations $Aut(G)$ form a group under composition. And this is a subgroup of the symmetric group of all permutations of the vertices $Sym(G)$

- Directions :
  - Fourier transforms are well defined over representations of non-abelian groups (matrices)
    - But Fourier basis transform gives us no interesting post measurement collapse
    - It’s shown impossible to solve HSP over Sym(G) using Fourier sampling [4]
  - There exist other “non-Fourier” quantum observables for GI - don’t know if implementable [3]

Non abelian HSPs

- Even in the most generic case of a determining a hidden subgroup K of an arbitrary group G, there are circuits that prepare a state where all possible subgroups hidden by a K periodic f are nearly orthogonal, and we *still can’t efficiently determine the generators of K*. (Problem 5.5 in course textbook)
    - The algorithm mentioned in [5] uses O(|G|) measurements.

References

1. Abstract Algebra: Theory and Applications - http://abstract.ups.edu/index.html
2. Quantum Theory, Groups and Representations: An Introduction - https://www.math.columbia.edu/~woit/QM/qmbook.pdf
3. A quantum observable for the graph isomorphism problem - https://arxiv.org/pdf/quant-ph/9901029.pdf
4. The symmetric group defies strong Fourier sampling - (I) https://arxiv.org/abs/quant-ph/0501056, (II) https://arxiv.org/pdf/quant-ph/0501066.pdf
5. Hidden subgroup states are nearly orthogonal https://arxiv.org/pdf/quant-ph/9901034.pdf
6. Quantum measurements and the Abelian Stabilizer Problem - https://arxiv.org/pdf/quant-ph/9511026.pdf
7. The quantum Fourier transform and extensions of the abelian HSP - https://arxiv.org/pdf/quant-ph/0212002.pdf