**Algebra and Computation** Course Instructor: V. Arvind

# Lecture 24: The Hidden Subgroup Problem

*Lecturer: V. Arvind* *Scribe: Ramprasad Saptharishi*

## 1 Overview

In this class we shall look at character theory and it's take on quantum computing. Once we have sufficient tools, we will get into the hidden subgroup problem, which can be used to solve a whole class of problems including the discrete logarithm.

## 2 The Hidden Subgroup Problem

The hidden subgroup problem is the natural generalization of the order finding problem.

*The Problem:* Let $G$ be a finite group and $H \leq G$ be a subgroup of $G$. Let $X$ be an arbitrary set and we are given a function $f : G \to X$ such that it is constant on every right coset of $H$ ($f(x) = f(y)$ if and only if $x$ and $y$ belong to the same right coset of $H$) and is different for different right cosets.

Find a generating set for $H$.

### 2.1 Discrete Log as a hidden subgroup problem

*Problem:* $p$ is a prime and $g$ is a generator for $\mathbb{Z}_p^\star$. Given $a \in \mathbb{Z}_p^\star$ find $x$ such that $g^x = a \pmod{p}$.

This can be easily converted to the HSP setting. Let $G'$ be the additive group $(\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}, +)$ and $f : G' \to \mathbb{Z}_p^\star$ such that it sends $(\alpha, \beta)$ to $g^\alpha a^{-\beta} \pmod{p}$.

It is easy to see that $(\alpha, \beta)$ goes to 1 if and only if $\alpha = x\beta$. Therefore, the hidden subgroup of this function is the subgroup generated by $(x, 1)$. Thus all we need to do is find a generator $(\alpha, \beta)$ and $\beta/\alpha = x$.

### 2.2 Graph Isomorphism as a hidden subgroup problem

We have seen earlier that graph isomorphism reduces to the problem of finding the automorphism group of the graph. Converting to the HSP setting is easy.

Let $\mathcal{G}_n$ be the set of all possible graphs on $n$ nodes. The hidden function is

$$\begin{aligned} f_X : S_n &\longrightarrow \mathcal{G}_n \\ \pi &\mapsto X^\pi \end{aligned}$$

that is, it takes a permutation and sends is to the graph obtained by permuting $X$ by that permutation.

The hidden subgroup is precisely the automorphism group of the graph.

This however is a case of the HSP in a non-abelian group setting. We will just solve the problem for finite abelian groups.

## 3 Characters of a finite group

A character of a finite abelian group $G$ is a homomorphism $\chi : G \rightarrow \mathbb{C}^\star$. That is, they satisfy properties like $\chi(1) = 1$,$\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$,$\chi(g^{-1}) = \overline{\chi(g)}$ etc.

Define $\mathbb{C}[G]$ to be the $|G|$ dimensional vector space over $\mathbb{C}$, by just consider the elements of $G$ as the standard basis elements of the vector space. It in fact also has a multiplicative structure and is called a group algebra. Note that the vector space for the quantum algorithms was $\mathbb{C}^{2^n} = \mathbb{C}[\mathbb{Z}_2^n]$ and at some points we even exploited the group structure of $\mathbb{Z}_2^n$. And the standard basis for the quantum setting were $\{|g\rangle \ : \ g \in G\}$ which is precisely $\mathbb{C}[G]$.

Now notice that $\mathbb{C}[G]$ can be thought of as a function from $\mathbb{C}$ to $G$, where every coordinate of the basis element can be thought of as the value of the function. Thus $\mathbb{C}[G] = \mathbb{C}^G$. In this setting, the characters, being functions from $G$ to $\mathbb{C}$, can be thought of as vectors in $\mathbb{C}[G]$.

### 3.1 Properties of Characters

- It is easy to see that for every $g \in G$, $\chi(g)^{|G|} = 1$ since $\chi$ is a homomorphism. Hence, $\chi(g)$ is a $|G|$-th root of unity.

  Thus characters are vectors where each coordinate is a $|G|$-th root of unity. The vector $(1, 1, \cdots, 1)$ is referred to as the trivial character.

- As in the quantum setting, we shall normalize characters by writing them as
$$|\chi\rangle = \frac{1}{\sqrt{G}} \sum_g \chi(g) \, |g\rangle$$
By the usual hermitian inner product ($\langle a|b\rangle = \sum \overline{a_i} b_i$), it is clear that $\langle \chi|\chi\rangle = 1$.

  Thus characters are vectors of norm 1.

- Suppose we have two distinct characters $\chi_1, \chi_2$, that is there exists an $h$ such that $\chi_1(h) \neq \chi_2(h)$. Let us look at what happens to $\langle \chi_1|\chi_2\rangle$ . Multiplying both sides by $\chi_1(h)$:
$$\begin{aligned}
\chi_1(h) \langle \chi_1|\chi_2\rangle &= \frac{1}{\sqrt{G}} \sum_g \chi_1(h)\chi_1(g^{-1})\chi_2(g) \\
&= \frac{1}{\sqrt{G}} \sum_g \chi_1(hg^{-1})\chi_2(g) \\
&= \frac{1}{\sqrt{G}} \sum_{\tilde{g}} \chi_1(\tilde{g}^{-1})\chi_2(\tilde{g}h) \quad , \quad \tilde{g} = gh^{-1} \\
&= \chi_2(h) \left( \frac{1}{\sqrt{G}} \sum_{\tilde{g}} \chi_1(\tilde{g}^{-1})\chi_2(\tilde{g}) \right) \\
&= \chi_2(h) \langle \chi_1|\chi_2\rangle
\end{aligned}$$
But since we assumed that $\chi_1(h) \neq \chi_2(h)$, this will force $\langle \chi_1|\chi_2\rangle = 0$. Thus the characters are mutually orthogonal to each other.

  And hence, for any non-trivial character $\chi$, $\langle (1, 1, \cdots, 1)|\chi\rangle = 0$ and hence $\sum_g \chi(g) = 0$.

Therefore it is clear that there are at most $|G|$ characters (a $|G|$ dimensional space can have at most that many mutually orthogonal vectors). For the finite abelian group setting, it is easy to show that there are in fact $|G|$ many characters.

**Theorem 1** (Structure theorem for finite abelian groups)**.** *Any finite abelian group $G$ is isomorphic to a direct product of cyclic groups.*

Thus
$$G \cong \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_l}$$

For a cyclic group $\mathbb{Z}_N$, it is easy to show that we indeed have $N$ characters:

$$\begin{aligned}
\omega_N &= e^{\frac{2\pi i}{N}} \\
\chi_j : \mathbb{Z}_n &\longrightarrow \mathbb{C}^\star \\
1 &\mapsto \omega_N^j \\
k &\mapsto \omega_N^{jk}
\end{aligned}$$

And clearly these are distinct. In the same way, we have $|G|$ distinct characters by just saying:

$$\chi_{j_1,j_2,\cdots,j_l}(a_1,a_2,\cdots,a_l) \mapsto (\omega_{N_1})^{j_1 a_1}(\omega_{N_2})^{j_2 a_2}\cdots(\omega_{N_l})^{j_l a_l}$$

Thus, the characters indeed form an orthonormal basis for $\mathbb{C}[G]$.

### 3.2 The fourier transform

The fourier transform is just the change of basis from the standard to the characters. And the transform played an important role in the order finding algorithm due to the property of 'shift invariance that the character basis enjoys.

$$\begin{aligned}
|\chi_g\rangle &= \frac{1}{\sqrt{G}}\sum_x \chi_g(x)\,|x\rangle \\
U_h\chi_g &= \frac{1}{\sqrt{G}}\sum_x \chi_g(x)\,|hx\rangle \\
&= \frac{1}{\sqrt{G}}\sum_x \chi_g(h^{-1})\chi_g(hx)\,|hx\rangle \\
&= \chi_g(h^{-1})\left(\frac{1}{\sqrt{G}}\sum_{x'}\chi_g(x')\,|x'\rangle\right) \quad , \quad x' = hx \\
&= \chi_g(h^{-1})\,|\chi_g\rangle
\end{aligned}$$

The fourier basis are all eigenvectors for all shift operators $U_h$, the eigenvalue being $\chi_g(h^{-1})$.

## 4 The Hidden Subgroup Problem for Finite Abelian Groups

The group is given to us as $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_l}$. And we need to find the hidden subgroup of $G$.

As in the Simon's problem and Shor's algorithm, first create the uniform superposition

$$|\psi\rangle = \frac{1}{\sqrt{G}} \sum_g |g\rangle$$

How we create this is a lovely trick that we shall see later in this lecture. Another thing we will assume that we can do a fourier transform (approximate at least) efficiently. Applying the function to the padded version, we get

$$\frac{1}{\sqrt{G}} \sum_g |g\rangle \, |f(g)\rangle$$

On measuring the second qubits, we would measure some $f(x)$ and thus would result in the state

$$\frac{1}{\sqrt{H}} \sum_h |xh\rangle$$

A fourier transform on this gives

$$\frac{1}{\sqrt{H}\sqrt{G}} \sum_h \sum_g \chi_{xh}(g) \, |g\rangle$$

Note that $\chi_a(b) = \chi_b(a)$. And hence

$$\begin{aligned} \frac{1}{\sqrt{H}\sqrt{G}} \sum_h \sum_g \chi_{xh}(g) \, |g\rangle &= \frac{1}{\sqrt{H}\sqrt{G}} \sum_h \sum_g \chi_g(xh) \, |g\rangle \\ &= \frac{\sqrt{H}\sqrt{G}}{\sum}_g \left( \sum_h \chi_g(h) \right) \chi_g(x) \, |g\rangle \end{aligned}$$

Now, since $\chi_g(h)$ is a character of $H$ as well the summation inside the bracket will be zero for a lot of $\chi$s.

At this point, for any group $G$, define the dual group $G'$ as the group of characters of $G$. $H^{\perp} = \{\chi \in G' \ : \ \chi(h) = 1 \forall h \in H\}$.

For all characters in $H^{\perp}$, the summation in the bracket will be $|H|$, and 0 otherwise. Hence the summation reduces to

$$\frac{\sqrt{H}}{\sqrt{G}} \sum_{g : \chi_g \in H^{\perp}} \chi_g(x) \, |g\rangle$$

Now measuring $|g\rangle$ will give us a random element in $H^{\perp}$. Thus using the sampling lemma in Simon's problem we can get a generating set for $H^{\perp}$. With this, how do we find a generating set for $H$?

Suppose we have our sample $g_1, g_2, \cdots, g_t$ where $t = 4\log|G|$. By the structure of the group $G$, $g_i = \langle a_{i_1}, a_{i_2}, \cdots, a_{i_l} \rangle$. Thus for each $x_i \in H$ we know that

$$\omega_{N_1}^{x_1 a_{i_1}} \omega_{N_2}^{x_2 a_{i_2}} \cdots \omega_{N_l}^{x_1 a_{i_l}} = 1$$

But this is an exponential constraint, if we have a linear constraint we can solve it using the techniques discussed earlier.

Let $N = lcm(N_i)$ and let $M_i = N/N_i$. Then the constraint above is just finding solutions $x_i$ to $\sum_j M_j a_{i_j} x_j = 0 \pmod{N}$. The mod can be removed as well by having an extra indeterminate $y_i$ and writing it as

$$M_1 a_{i_1} x_1 + M_2 a_{i_2} x_2 + \cdots M_l a_{i_l} x_l + N y_i = 0$$

These constraints, for each $i$, is just a system of diophantine equations that can be solved using the hermite normal form. Thus, this would solve the hidden subgroup problem.

### 4.1 The Converse

Another important question is the following: suppose we have a way of solving the hidden subgroup problem for a finite abelian group, can we use that to find the structure of $G$?

One way is to take the generators of $G$ (by random sampling), finding their orders and factorizing them. The factorization of the orders will decompose the group in to a direct product of $p$-groups. How do we find the cyclic product decomposition of the $p$-groups?

We shall discuss this in the next lecture.

### 4.2 Creating the uniform superposition

We want to create the state

$$|\psi\rangle = \frac{1}{\sqrt{G}} \sum_g |g\rangle$$

The idea is to find a binary encoding of the group and use that. Encode elements of $G$ using binary strings of length $m$, $m$ chosen such that $2^m \geq |G| \geq 2^m/poly(m)$ (a reasonably efficient encoding). Once we have an encoding function, we naturally have another checker functions $U_f$ that takes a binary string and decides whether it is actually an encoding of an element of $G$.

Using the hadamard transform, we can create a uniform superposition over $\{0,1\}^m$:

$$|\psi\rangle = \frac{1}{2^m} \sum_{x \in \{0,1\}^m} |x\rangle$$

Applying the checker function to the padded version of this, we get

$$\frac{1}{2^m} \sum_{x \in \{0,1\}^m} |x\rangle \, |f(x)\rangle$$

Now since we assumed that the encoding is reasonably efficient, measuring $f(x)$ will give us a 1 with high probability. And hence, the rest of the state will collapse to

$$\frac{1}{\sqrt{G}} \sum_{g} |g\rangle$$

which is precisely what we want!