The Hidden Subgroup Problem

CSE 490Q: Quantum Computation
Shor’s Algorithm

• Shor’s (1994) breakthrough result was an efficient q. algorithm for factoring
  • strongly believed to be classically hard
    • 200+ years of failed attempts to solve it
    • hardness is assumed by cryptosystems like RSA
  • not a toy problem, not a black box

• Fastest classical algorithm runs in $O(2^{n/3})$ time
• Shor’s algorithm is $O(n^3)$
• Much later work focused on *generalizing* it
  • we will look at some of the generalizations (more than one!)
  • Shor’s paper still has insights that may not be fully understood still

• First generalization was the phase estimation algorithm

• Second generalization is...
**Problem**: Given a function $f : G \rightarrow \{0,1\}^k$ (via an oracle) that is constant on cosets of some subgroup $H$, find the subgroup $H$.

- What does all that mean?
Definition: A group $G$ is a set with...

- a special element $e \in G$
- an operation taking any $x, y \in G$ to some $xy \in G$
- an operation taking any $x \in G$ to some $x^{-1} \in G$

satisfying certain rules...

- $ex = x = xe$ for all $x \in G$ ("identity")
- $xx^{-1} = e = x^{-1}x = e$ for all $x \in G$ ("inverses")
- $(xy)z = x(yz)$ for all $x, y, z \in G$ ("associativity")

Definition: A group $G$ is abelian if $xy = yx$ for all $x, y \in G$.

- (In this case, we often write $x+y$ instead of $xy$.)
A subgroup is a subset of a group that is itself a group (with the same operations).

In particular, $S \subseteq G$ is a subgroup iff

- $e \in S$
- if $x \in S$, then $x^{-1} \in S$
- if $x \in S$ and $y \in S$, then $xy \in S$

So you can perform group operations on elements of $S$ and you will never see an element outside of $S$ (i.e., from $G - S$).
• If $S \subseteq G$ is a subgroup, then a **coset** of $S$ is a set of the form

$$gS = \{ gs : s \in S \}$$

for some $g \in G$.

• This is not a subgroup (e.g., we do not have $e \in gS$). It is just a subset of $G$.

• The cosets of $S$ **partition**, so we can write

$$G = g_1S \cup g_1S \cup ... \cup g_kS$$

for some choice of $g_1, ..., g_k \in G$. 
**Problem:** Given a function $f : G \to \{0,1\}^k$ (via an oracle) that is **constant on cosets** of some subgroup $H$, find the subgroup $H$.

- I.e., we are promised that $f(gh_1) = f(gh_2)$ for all $h_1, h_2 \in H$ and $g \in G$.
- Equivalently, $f(g) = f(gh)$ for all $h \in H$ and $g \in G$.
- Outputs need not have any meaning.
- Requires exponential time classically.

$\mathcal{G} \subseteq \mathbb{Z}_p \times \mathbb{Z}_q$
Shor’s paper solved another problem called “discrete logarithm”

**Definition**: Given $b, d \in \mathbb{Z}_p$, find an $r \in \mathbb{Z}_{p-1}$ such that $b^r \equiv d \pmod{p}$

- If these were real numbers, we would have $r = \log_b(d)$, but this is $\mathbb{Z}_p$.

- Strongly believed to be hard classically
  - e.g., the Diffie-Hellman key exchange protocol uses this assumption
**Definition:** Given $b, c \in \mathbb{Z}_p$, find an $r \in \mathbb{Z}_{p-1}$ such that $b^r \equiv d \pmod{p}$

- Solve the HSP over $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ with the following hiding function
  \[ f(x, y) = b^x (d^{-1})^y \pmod{p} \]

- (We can find $d^{-1}$ efficiently by Euclid’s algorithm.)

- Can see that $f(r, 1) = b^r (d^{-1})^1 = b^r d^{-1} \equiv 1 \pmod{p}$

- More generally, $f(kr, k) = b^{kr} (d^{-1})^k = (b^r d^{-1})^k \equiv 1^k = 1 \pmod{p}$
**Definition:** Given $b, c \in \mathbb{Z}_p$, find an $r \in \mathbb{Z}_{p-1}$ such that $b^r \equiv d \pmod{p}$

- Solve the HSP over $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ with the following hiding function

  $$f(x, y) = b^x (d^{-1})^y \pmod{p}$$

- We can see that $f(kr, k) = b^{kr} (d^{-1})^k = (b^r d^{-1})^k \equiv 1^k = 1 \pmod{p}$

- $f$ is constant $(1)$ on the subset $H = \{(kr, k) : k \in \mathbb{Z}_{p-1}\}$
  - can check that $H$ is a group
  - can check that $f$ is constant on all cosets of $H$
**Definition:** Given \( b, c \in \mathbb{Z}_p \), find an \( r \in \mathbb{Z}_{p-1} \) such that \( b^r \equiv d \pmod{p} \)

- Solve the HSP over \( \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \) with the following hiding function

\[
 f(x, y) = b^x (d^{-1})^y \pmod{p}
\]

- Solving the HSP will give us a generator \( (a, k) \in H = \{ (kr, k) : k \in \mathbb{Z}_{p-1} \} \)

- The answer is \( k^{-1} a = k^{-1} kr = r \)
Kitaev solved this problem (essentially) for all abelian groups.

We will see the modern solution shortly.

First, we need a bit more background on groups...
Characters
• Working with $G = \mathbb{Z}_N$, consider these functions:

$$\chi_j(k) = e^{\frac{2\pi i j k}{N}}$$

for $j \in \mathbb{Z}_N$

• They have the properties that

$$\chi_j(x+y) = e^{\frac{2\pi i j (x+y)}{N}} = e^{\frac{2\pi i j x}{N} + \frac{2\pi i j y}{N}} = e^{\frac{2\pi i j x}{N}} e^{\frac{2\pi i j y}{N}} = \chi_j(x) \chi_j(y)$$

and

$$\chi_j(0) = e^0 = 1$$
Exponentials

• Working with $G = \mathbb{Z}_N$, consider these functions:

$$\chi_j(k) = e^{2\pi i j k / N}$$

for $j \in \mathbb{Z}_N$

• They have the properties that
  • $\chi_j(x+y) = \chi_j(x) \chi_j(y)$
  • $\chi_j(0) = 1$
A function $\chi : G \to \mathbb{C}$ is called a “character of $G$” if it satisfies

- $\chi(xy) = \chi(x) \chi(y)$
- $\chi(e) = 1$

The “irreducible” characters of $\mathbb{Z}_N$ are $\chi_0, \chi_1, \ldots, \chi_{N-1}$
A function $\chi : G \rightarrow \mathbb{C}$ is called a "character of $G$" if it satisfies
- $\chi(xy) = \chi(x) \chi(y)$
- $\chi(e) = 1$

The "irreducible" characters of $\mathbb{Z}_N$ are $\chi_0, \chi_1, \ldots, \chi_{N-1}$

The set of irreducible characters is often denoted $\hat{G}$ (or $G^\wedge$)
- we have $|\hat{G}| = |G|$ (or $G^\wedge$)
- nearly all the information about the group is also in its characters
Properties of Characters

• It can be shown that, for any two distinct irreducible characters $\chi$ and $\gamma$, we have

$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \gamma(g) = \begin{cases} 1 & \text{if } \chi = \gamma \\ 0 & \text{otherwise} \end{cases}$$

and for any distinct elements $g, h \in G$, we have

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \overline{\chi(g)} \chi(h) = \begin{cases} 1 & \text{if } g = h \\ 0 & \text{otherwise} \end{cases}$$

• For $\mathbb{Z}_N$, these are calculations involving exponentials that we did already...
Properties of Characters

• For $\mathbb{Z}_N$, these are calculations involving exponentials that we did already:

$$\sum_{x=0}^{N-1} \chi_j(x) \chi_k(x) = \sum_{x=0}^{N-1} e^{2\pi i j x/N} e^{2\pi i k x/N}$$

$$= \sum_{x=0}^{N-1} e^{2\pi i (k-j) x / N} = \sum_{x=0}^{N-1} \left( e^{2\pi i (k-j)/N} \right)^x$$

$$= \omega^0 + \omega^1 + \omega^2 + \cdots + \omega^{N-1} \text{ where } \omega = e^{2\pi i (k-j)/N}$$

$$= \begin{cases} 
\frac{N}{k=j} & \text{if } \omega = 1 \\
0 & \text{otherwise} \end{cases}$$
Since we want

\[ \sum_{g \in \mathcal{G}} \overline{\chi(g)} \gamma(g) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} \]

we need to rescale by \( N^{-1/2} \) so that we have

\[ \chi_j(k) = \frac{1}{\sqrt{N}} e^{2\pi i j k / N} \]
Quantum Fourier Transform
We will work in a basis labeled by group elements: \( \{ |g\rangle : g \in G \} \)

- need \( \log_2(G) \) qubits
- choose any convenient mapping between bits and group elements

Can also have a basis labeled by characters: \( \{ |\chi\rangle : \chi \in G^\wedge \} \)

- exactly the same size
- choose any convenient mapping of bits to character names
The QFT $F$ is a change of basis from group elements to characters:

$$F |g\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi(x) |x\rangle$$

- Takes a group element to a vector of its character values
- This is a matrix whose columns are the characters
- Hence, this is unitary by column orthogonality
• When $G = \mathbb{Z}_N$, the characters are the functions

$$\chi_j(k) = e^{2\pi i j k / N} \quad \text{for } j \in \mathbb{Z}_N$$

• So the QFT is

$$\mathcal{F}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$$

which is exactly our definition from before of “the QFT” with $N = 2^n$. 

QFT Example 1
• When $G = \mathbb{Z}_N$, the characters are the functions

$$\chi_j(k) = e^{2\pi i j k / N} \quad \text{for } j \in \mathbb{Z}_N$$

• If $N = 2$, then the two characters are...

$$\chi_0(k) = e^0 = 1$$

$$\chi_1(k) = e^{2\pi i k / 2} = e^{\pi i k} = (e^{\pi i})^k = (-1)^k$$
• When $G = \mathbb{Z}_N$, the characters are the functions

$$\chi_j(k) = e^{\frac{2\pi i j k}{N}} \quad \text{for } j \in \mathbb{Z}_N$$

• If $N = 2$, then the two characters are
  • $\chi_0(k) = 1$
  • $\chi_1(k) = (-1)^k$

• So the Fourier transform is...

  i.e., the Hadamard gate!
QFT Example 2

- When $G = \mathbb{Z}_2$, the characters are $\chi_0(k) = 1$ and $\chi_1(k) = (-1)^k$

- For a product group $G_1 \times G_2$, the characters are products of the form

  $$\chi(g_1, g_2) = \chi(g_1) \chi(g_2)$$

  for some $j, k$

- For $\mathbb{Z}_2 \times \mathbb{Z}_2$, there are four elements and four characters

  $f = \frac{1}{2} \begin{pmatrix}
  \chi_0 & \chi_{x_1} & \chi_{x_2} & \chi_{x_1 x_2} \\
  \chi_{x_0} & \chi_{x_1} & \chi_{x_0 x_1} & \chi_{x_0 x_1 x_2} \\
  \chi_{x_1} & \chi_{x_0 x_1} & \chi_{x_0 x_1 x_2} & \chi_{x_1 x_2} \\
  \chi_{x_0 x_1 x_2} & \chi_{x_0 x_1 x_2} & \chi_{x_0 x_1} & \chi_{x_1} \\
  \end{pmatrix} = H \otimes H$

  $H = \begin{bmatrix}
    1 & 1 \\
    1 & -1 \\
    1 & -1 \\
    1 & 1 \\
  \end{bmatrix}$
More generally, the QFT for $G = (\mathbb{Z}_2)^n = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ is $H^\otimes n$

So all of our algorithms using $H^\otimes n$ are using QFTs.

In particular, Deutsch-Josza used the QFT over $(\mathbb{Z}_2)^n$.
Then, Shor used the QFT over $\mathbb{Z}_N$.
Now, we realize that these are just QFTs over different abelian groups.
HSP for Abelian Groups
For all abelian groups (and some non-abelian ones), we can solve the HSP using the following procedure...

1. Prepare the state

\( \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |0\rangle \right) \)

\( = F^t |x_0\rangle \otimes |0\rangle \)
1. Prepare the state

\[ \frac{1}{\sqrt{14!}} \sum_{g \in \mathcal{g}} |g\rangle \otimes |0^k\rangle \]

2. Apply $U_f$ to the second register giving us

\[ \frac{1}{\sqrt{14!}} \sum_{g \in \mathcal{g}} |g\rangle \otimes |f(g)\rangle \]

3. Measure (and discard) the second part of the state...
3. Measure (and discard) the second part of the state...

- Recall that $G$ can be partitioned by cosets into

$$G = g_1H \cup g_2H \cup \ldots \cup g_kH$$

for some choice of $g_1, \ldots, g_k \in G$.

- Recall that $f(gh) = f(g)$ for all $h \in H$ since $f$ is constant on cosets.
The “Standard” Solution

\[ \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g \rangle \otimes |f(g)\rangle \]

3. Measure (and discard) the second part of the state...

Since \( G = g_1H \cup g_1H \cup ... \cup g_kH \), the state above is

\[ \frac{1}{\sqrt{|G|}} \left( |g_1 h_1 \rangle \otimes |f(g_1, h_1)\rangle + \ldots + |g_{k-1} h_{k-1} \rangle \otimes |f(g_{k-1}, h_{k-1})\rangle + |g_k h_k \rangle \otimes |f(g_k, h_k)\rangle \right) \]
The “Standard” Solution

\[
\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle
\]

3. Measure (and discard) the second part of the state...

Since \( G = g_1H \cup g_1H \cup ... \cup g_kH \) and \( f(gh) = f(g) \) for all \( h \in H \), the state above is

\[
\frac{1}{\sqrt{|G|}} \left( |g_1h_1\rangle \otimes |f(g_1)\rangle + \ldots + |g_1h_{_x}\rangle \otimes |f(g_{_1})\rangle + \ldots + |g_kh_r\rangle \otimes |f(g_k)\rangle \right)
\]
The “Standard” Solution

\[ \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle \]

3. Measure (and discard) the second part of the state...

Since \( G = g_1H \cup g_1H \cup ... \cup g_kH \) and \( f(gh) = f(g) \) for all \( h \in H \), the state above is

\[ \frac{1}{\sqrt{|C_g|}} \left( \left( |g_1h_1\rangle + ... + |g_1h_{r_1}\rangle \right) \otimes |f(g_1)\rangle + \ldots \right) \]

\[ \left( \left( |g_kh_1\rangle + ... + |g_kh_{r_k}\rangle \right) \otimes |f(g_k)\rangle \right) \]
3. Measure (and discard) the second part of the state...

\[
\frac{1}{\sqrt{|C_0|}} \sum_{g \in C_0} |g\rangle \otimes |f(g)\rangle
\]

We will get one of \(|f(g_1)\rangle + \ldots + |f(g_k)\rangle\), uniformly at random.
The “Standard” Solution

\[ \frac{1}{\sqrt{\sum_{g \in \mathcal{C}_t}}} \left( \sum_{g \in \mathcal{C}_t} |g\rangle \otimes \psi(g) \right) \]

3. Measure (and discard) the second part of the state...

\[ \frac{1}{\sqrt{\sum_{g \in \mathcal{C}_t}}} \left( |g_1h_1\rangle + \ldots + |g_kh_k\rangle \right) \otimes \psi(g_i) \]

for a uniformly random \( i = 1, \ldots, k \)

- The function value has no meaning, so we discard it.
3. Measure (and discard) the second part of the state...

\[
\frac{1}{\sqrt{|H|}} \left( \sum_{i=1}^{k} |g_i h_i \rangle + \ldots + |g_i h_k \rangle \right)
\]

for a uniformly random \(i = 1, \ldots, k\).

4. Apply the QFT for G to get

\[
\mathcal{F} \left( \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh \rangle \right) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi(g h) |1x \rangle
\]

\[
= \frac{1}{\sqrt{|G||H|}} \sum_{x \in C} \chi(g) \left( \sum_{h \in H} \chi(h) \right) |1x \rangle
\]
4. Apply the QFT for G to get

\[
\mathcal{F}\left( \frac{1}{\sqrt{|H|}} \sum_{h \in H} 1_{\text{gh}} \right) = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi(\text{gh}) |x\rangle \\
= \frac{1}{\sqrt{|G|}} \sum_{x \in G} \sum_{h \in H} \chi(g) \chi(h) |x\rangle \\
= \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi(g) \left( \sum_{h \in H} \chi(h) \right) |x\rangle
\]

5. Measure this to get some \( \chi \).
4. Measure this to get some $\chi$.

- The probability of measuring $\chi$ is given by

$$\frac{\left| \chi(g) \right|^2}{\left| G \right| \left| H \right| \left( \sum_{h \in H} \left| \chi(h) \right|^2 \right)}$$
The “Standard” Solution

• The probability of measuring $\chi$ is given by

$$\frac{|\chi(g)|^2}{|G| |H|} \left| \sum_{h \in H} \chi(h) \right|^2$$

• It is always the case that $\chi(g) = \chi(g^{-1})$

• So we have $|\chi(g)|^2 = \chi(g^{-1}) \chi(g) = \chi(g^{-1} g) = \chi(e) = 1$

• Hence, we can simplify this to...
The “Standard” Solution

• The probability of measuring $\chi$ is given by

$$\frac{1}{|G|} \left| \sum_{h \in H} \chi(h) \right|^2$$

• Note that $\chi$ is also a character of $H$ (since it satisfies $\chi(h_1 h_2) = \chi(h_1) \chi(h_2)$), so

$$\chi(s, t^2) = \chi(s) \chi(t^2)$$

$$\chi(1, g) = 1 \quad \text{if } \chi \equiv 1 \text{ on } H$$

$$= \begin{cases} 1 & \text{if } \chi \equiv 1 \text{ on } H \\ 0 & \text{otherwise} \end{cases}$$
The “Standard” Solution

• The probability of measuring $\chi$ is given by

$$\frac{1}{|G| |H|} \left| \sum_{h \in H} \chi(h) \right|^2$$

• Unless $\chi \equiv 1$ on $H$, this is probability is 0.
• When $\chi \equiv 1$ on $H$, the probability is

$$\frac{1}{|G| |H|} \left| \sum_{h \in H} 1 \right|^2 = \frac{|H|^2}{|G| |H|} = \frac{|H|}{|G|}$$
The result of this calculation is an element of the set of irreducible characters of G that are **trivial** on H.

In other words, we have $H \subseteq \text{Ker}(\chi) = \{ g \in G : \chi(g) = 1 \}$

To solve the problem, we do this multiple times and get $\chi_1, \ldots, \chi_t$.

H must be contained in all of their kernels, so we have $H \subseteq \text{Ker}(\chi_1) \cap \ldots \cap \text{Ker}(\chi_t)$. 
The “Standard” Solution

- Perform this calculation multiple times and get $\chi_1, \ldots, \chi_t$.

- $H$ must be contained in all of their kernels, so we have $H \subseteq \text{Ker}(\chi_1) \cap \ldots \cap \text{Ker}(\chi_t)$.

- It can be shown (with more character theory), that each new character that we measure shrinks the size of $\text{Ker}(\chi_1) \cap \ldots \cap \text{Ker}(\chi_t)$ by at least a factor of 2.
  - easy to check for the exponentials:
    - we only have $\chi_j(x) = 1$ if $xj$ is a multiple of $N$
    - this is most likely if $N$ is even and $x = N/2$, in which it holds for half of $j$’s

- Hence, the intersection converges to $H$ after a small number of samples
Perform this calculation multiple times and get $\chi_1, \ldots, \chi_t$.

$H$ must be contained in all of their kernels, so we have $H \subseteq \text{Ker}(\chi_1) \cap \ldots \cap \text{Ker}(\chi_t)$.

The intersection converges to $H$ after a small number of samples.

It remains to show how to perform this set intersection:
- in general, this depends on the details of the group
- however, for abelian groups, which are just $\mathbb{Z}_{N_1} \times \ldots \times \mathbb{Z}_{N_k}$, this turns out to be a straightforward, classical calculation
  - (similar to Gaussian elimination)
• Solution to the HSP for all abelian groups
  • solves factoring and discrete logarithm as special cases
  • more general and cleaner than prior solutions

• Next time: non-abelian groups
  • will be higher level (and shorter)