# Lecture 17: The Hidden Subgroup Problem

(All the cool quantum algs. we've seen so far were quite similar: similar problem & similar solution. Today we want to distill & generalize the problem, which could hopefully lead to more exponentially-faster quantum algs.)

Task: ① Bernstein-Vazirani: "given" $F: \{0,1\}^n \to \{0,1\}$, $F(X) = S \cdot X$, find $S$.

($\cdot$ = mod-2/$\mathbb{F}_2^n$ dot product)

[Via a q. circuit $Q_F$ implementing it.]

② Simon's Problem: given $F: \{0,1\}^n \to$ COLORS, $L$-periodic ($L \in \{0,1\}^n$): $F(X) = F(X \oplus L)$; (otherwise distinct) find $L$.

③ Period-Finding: given $F: \mathbb{Z}_N \to$ COLORS, $L$-periodic: ($L$ divides $N$) $F(X) = F(X+L) = F(X+2L) = \ldots$, find $L$.

(④ Shor's Order-Finding) ($X + kL$ happens "in $\mathbb{Z}$" – no wraparound)

Quantum Alg: (In brief...)

"efficient" $\approx n^{\text{const.}}$ gates.

- "Loaded" F into n-qubit state
- Did a Fourier transform, got a "clue".
- Classically converted clue(s) to solution.

[[ Today we'll talk about... ]]

① Common generalization of the task:

HSP = Hidden Subgroup Problem

② Can we always solve it efficiently on a quantum computer? [[ New Fourier transforms? New "clue-decoding" methods? Or...? ]]

③ Would solving different HSP variants be useful?! [[ For anything interesting? ]]

① • Set $\{0,1\}^n$, operation $\oplus$ (xOR)

• Set $\mathbb{Z}_N$, operation + mod N

• Set $\mathbb{Z}$, operation +

Each pair here is a "group" (commutative, in fact).

[[ A certain kind of algebraic structure you might know a bit about. We'll talk a bit about... ]]

e.g. HSP over...

$\mathbb{Z}_{24} = \{0,1,2,\ldots 23\}$, + (mod 24)

"secret" → "Subgroup generated by 4" (think "L=4")

$H := \{0, 4, 8, 12, 16, 20\}$

$(0+4)\ (4+4)\ (8+4)$

[[ that's it ]]

"Cosets (= "translates") of H":

"1+H" = {1, 5, 9, 13, 17, 21}

"2+H" = {2, 6, 10, 14, 18, 22}

"3+H" = - - - -

[[ That's it. Well, there's "0+H" ]]

Problem: $F: \mathbb{Z}_{24} \to$ COLORS is "H-periodic".

"Find H." [[ Like "Period-Finding", L=4. ]]

## ② Quantumly efficiently solvable?

**Case 1:** Commutative groups. [[ $X+Y=Y+X$ ]]

→ Yes! [[ Using combinations of techniques we've already seen. ]]

**Case 2:** Non-commutative. [[ E.g., "symmetric group", the set of all permutations of $\{1,2,\ldots,n\}$. ]]

↳ • Load. ✓

• "Fourier Transform"?

↳ • exists [[ complicated tho, uses "group representation theory" ]]

• People have shown it's doable efficiently on Q.C. for most interesting groups [[ Hard work over last 20 years ]]

• Fourier sampling "clues" → ??? → secret periodicity $H$

Not known to be efficiently doable in almost any case. ☹

Known [EHK] (future lecture) that, information-theoretically, poly(n) many "clues" suffice! [[ Don't know how to solve the crime computationally efficiently, tho. ]] 😕

## ③ Useful? Yes!!

| HSP for Group | Application |
|---|---|
| $\{0,1\}^n$, XOR / $\mathbb{F}_2^n$ | Simon's Alg. → pedagogy ☺ |
| $\mathbb{Z}_N$, + | Period-Finding " |
| " $\mathbb{Z}$ ", + | Shor's Factoring |
| $\mathbb{Z}_N \times \mathbb{Z}_N$, + | Shor's Discrete Log Alg. (very sim. to Factoring; breaks crypto like Diffie-Hellman) |
| " $\mathbb{R}$ ", + | implicitly solving Pell's equation ☹ [Hallgren'00] |

‖ For $\mathbb{Z}$ (Shor) & $\mathbb{R}$, you ultimately discretize to $\mathbb{Z}_N$, use $DFT_N$ ‖

commutative & done!

‖ OTOH, for noncommutative groups, there would be spectacular consequences... but we don't know how to efficiently do HSP quantumly in these cases ☹ ‖

| HSP for group | Application |
| --- | --- |
| "dihedral group"<br>[[Kuperberg has a $\approx 2^{\sqrt{n}}$ quantum alg.; compared to $\sqrt{2}^n$ classical]] | "approximate shortest vector in a lattice" problem<br>[Regev] [[The foundational presumed hard problem for "post-quantum cryptography"]] |
| "symmetric group"<br>(reduction will be on homework)<br>[[So crazy that these problems... factoring, discrete log, SVP, GISO,... are all of the super-rare "not known in P, nor NP-complete type". Tantalizing...]] | Graph-Isomorphism<br>[[A famous problem not known to be "in P", & almost surely not "NP-complete". Babai did it classically in $n^{\text{polylog}\,n}$ time a few years ago, famously; but believes $n^{\log n} \gg P$ is required. Could quantum do it in poly time??]] |

# Groups, briefly

Def: a set $G$ [[think finite, for simplicity]]
& a binary operation $\circ : G \times G \to G$

s.t. ① "$x \circ y \circ z$ makes sense":

$$x \circ (y \circ z) = (x \circ y) \circ z$$ [[associative]]

② $\exists$ a "neutral" element $e \in G$:

$$e \circ x = x, \quad x \circ e = x \quad \forall x \in G$$

③ $\forall x \in G \ \exists$ "inverse" $x' \in G$ s.t.

$$x \circ x' = x' \circ x = e.$$

Need not have "$\circ$ is commutative": $x \circ y = y \circ x$.

# Commutative Group E.g.'s

- $G = \{0,1\}^n$, $\circ$ = XOR (component-wise)
  $e = (0, 0, \ldots, 0)$
  $x' = x$

  Same as $G = \mathbb{F}_2^n$, $\circ = +$ (comp-wise) mod 2

- $G = \mathbb{Z}_N$, $\circ = +$ mod $N$, $e = 0$, $x' = -x$.
- $G = \mathbb{Z}_B^*$, $\circ = \cdot$ mod $N$, $e = 1$, $x' = x^{-1}$
- $G = \mathbb{Z}_N \times \mathbb{Z}_N$, $\circ = +$ mod $N$ (componentwise)
  [Shor's Discrete Log] $e = (0,0)$. $(x,y)' = (-x,-y)$.

Fact: every finite commutative group is same as $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_k}$, operation $+$

Infinite e.g.: $G = \mathbb{Z}$, $\circ = +$ ; $G = \mathbb{R}$, $\circ = +$

# Non-commutative e.g.s:

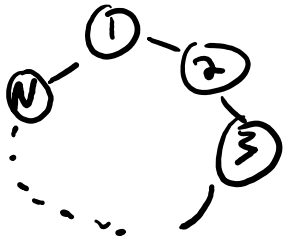
- "Symmetric group $S_n$" [[ for graph isomorphism ]]
  - $G$ = all permutations $\pi : \{1, 2, \ldots, n\} \to \{1, \ldots, n\}$.
    $\circ$ = "composition" $\pi_1 \circ \pi_2$ = do $\pi_2$, then do $\pi_1$
    $e$ = $\pi(i) = i$ $\forall i$. $\pi'$ = inverse of $\pi$.

Not commutative:

$$\begin{matrix} 1\to2 \\ 2\to1 \\ 3\to3 \end{matrix} \circ \begin{matrix} 1\to2 \\ 2\to3 \\ 3\to1 \end{matrix}$$

Right first, then left:
$1\to1, 2\to3, 3\to2$.
other way:
$1\to3, 2\to2, 3\to1$

- "Dihedral group $D_N$"
  - $G$ = perms $\pi : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, N\}$ that are "automorphisms" (self-isomorphisms) of the $N$-cycle graph




$|G| = 2N$: $N$ "reflections", $N-1$ nontrivial "rotations"
$1$ neutral $e$ = do nothing

## Subgroups: (E.g.: $G = \mathbb{Z}_{24}$, $op = +$).

Take an element $h \in G$. (E.g., $h = 4$.)

Subgroup generated by $h$ is

$H := \{e, h, h \circ h, h \circ h \circ h, \ldots, h', h' \circ h', \ldots\}$

(E.g.: $H = \{0, 4, 8, 12, 16, 20\}$.)

"Starting from $e$, do $\circ$ with $h, h'$ as much as possible".

[["Subgroup" b/c it's a subset, & is itself a group]]

Can also have subgroups generated by two elts. $h_1, h_2 \in G$ (or 3, 4, etc...)

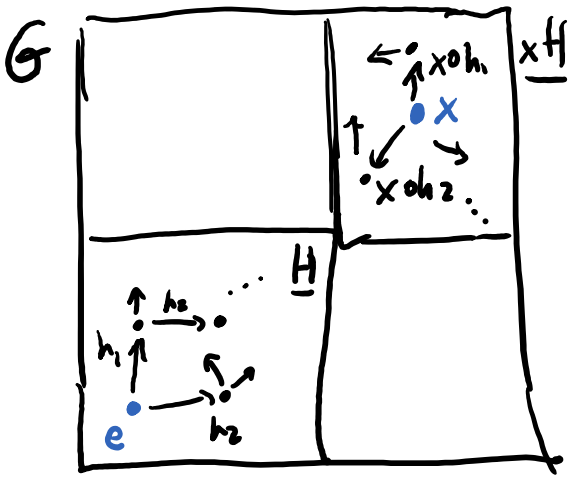
$H := \{e, h_1, h_2, h_1 \circ h_1, h_1 \circ h_2, h_2 \circ h_2, h_1', h_2', \ldots \text{ etc.}\}$

[[again: "starting from $e$, combine $h, h'$ with $\circ$ as much as possible"]]

eg: Dihedral group $D_n$ is subgroup of symmetric group $S_n$ generated by "rotation" $1 \to 2, 2 \to 3, \ldots, n \to 1$ & "reflection" $1 \to n, n \to 1, 2 \to n-1, n-1 \to 2, \ldots$.

# Cosets := "translates of subgroups"

Say $H$ is subgroup generated by $h_1, h_2 \in G$.




"Coset of $H$ with translate ("representative") $x \in G$" denoted "$xH$", is "start at $x \in G$, apply $\circ$ with $h_1, h_1', h_2, h_2'$ as much as possible".

[["Looks pretty much same as $H$, but "translated" by $x$."]]

e.g.: $G = \mathbb{Z}_{24}, +$. $H$ gen'd by 4, $H = \{0,4,8,12,16,20\}$.

Coset with translate $x=1$: $xH = \{1,5,9,13,17,21\}$

" " $x=2$: $\{2,6,10,14,18,22\}$

$=3$: $\{3,7,\ldots\}$

" " $x=4$: $xH = H$

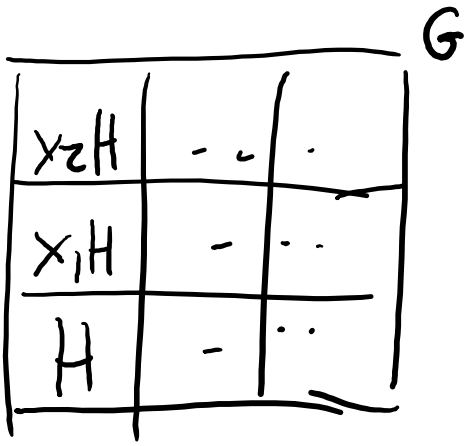
$x=5$: same as $x=1$

$x=6$: " " $x=2$.

. . .

## Simple facts (exercises!)

- $|xH| = |H|$ for all $x \in G$
- any two cosets $xH$, $yH$ are either identical, or disjoint
- {cosets of $H$} partition $G$




**Def:** $F: G \to$ colors is "H-periodic"

(( nonstandard name; maybe "F is H-coset preserving..." ))

if:
- for each coset $xH$, $F$ has same val. on all elts.
  ("$F(x) = F(x \circ h_1) = F(x \circ h_2) = F(x \circ h_1 \circ h_2) = \ldots$")
- $F$ gives different cosets different colors.

# Hidden Subgroup Problem for $G$, $\circ$ ($HSP_G$)

Given quantum circuit $Q_F$ implementing some $H$-periodic $F: G \to \text{COLORS}$,

find $H$.

↑ find generators for $H$.

↖ assume $x \in G$ represented by $\wedge \approx \log |G|$ bits

E.g.:

- Simon's Problem: ⟦promised to be just 1 generator⟧

  $G = \mathbb{F}_2^n$, $H$ generated by a single $L \in \mathbb{F}_2^n$,

  $H = \{0, L\}$. Cosets are $\{X, X+L\}$.

- Bernstein-Vazirani: $H = \{X : X \cdot S = 0\}$ for some secret $S$.

  Only two cosets: $H$ & $\{X : X \cdot S = 1\}$.

- Period-Finding over $\mathbb{Z}_N, +$:

  $H$ generated by "secret" $L$: $L/N$

  $\{0, L, 2L, \cdots\}$.

  Cosets are $\{X, X+L, X+2L, \cdots\}$.

# Trying to solve $HSP_G$, quantumly

## The "standard method"

[Official name for Simon's method... ]

① Prepare unif. superposition:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle.$$

② Attach "output register" $|0\rangle$'s, pass thru $Q_F$, get

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

③ Measure output register.

Get some color $C^*$

$F$ uses $\frac{|G|}{|H|}$ different colors, each equally often.

State collapses to

$$\frac{1}{\sqrt{|H|}} \sum_{x : F(x)=C^*} |x\rangle|C^*\rangle$$

($|C^*\rangle$: trash)

$$\updownarrow \text{ equiv: } \sum_{x \in gH} \text{ for some } \underline{\text{random}} \text{ coset } gH.$$

[Technically... if $|G|=N$, presumably you have a system for rep'ing each $x \in G$ by $n \approx \lceil \log N \rceil$ bits. A (non-huge) fraction of $\{0,1\}^n$ will not correspond to any $x \in G$, but it'll be ok. Just make $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$. ]

[Assume $F(x) =$ "NULL" ∉ COLORS if $x \in \{0,1\}^n$ doesn't encode a group elt. ]

[If you measure the "color" NULL, just restart until you get a proper color. ]

$\frac{1}{\sqrt{|H|}} \sum_{x \in gH} |x\rangle =: "|gH\rangle"$ is called a

coset state.

We actually get a (uniformly) random coset state.

Rec: A probability distribution over ("pure") quantum states is call a "mixed quantum state".

[ It's the real real notion of quantum states. We'll study them soonish. ]

"$\rho_H$" = uniform distribution over all coset states $|gH\rangle$.

We can "create" the mixed state $\rho_H$ efficiently. Can we learn $H$ from it?

"Standard" idea: Apply the "appropriate" Fourier transform for $G$ & measure.

"Fourier sampling" paradigm.

Gives a "clue" about $H$.

Hopefully can deduce $H$.

Fact: · All commutative (finite) $G$ of form $\mathbb{Z}_{N_1} \times \cdots \times \mathbb{Z}_{N_k}$.

· Appropriate Fourier Transform is $DFT_{N_1} \otimes \cdots \otimes DFT_{N_k}$.

· Efficiently implementable, quantumly

Combo of ideas we've seen solves $HSP_G$ in any commutative $G$. ☺

## Noncommutative groups (e.g. $S_n$, $D_N$)

- appropriate "Fourier transform"
  - → mathematically complicated
  - → nevertheless, shown to be efficiently quantumly doable in most cases

- But! : Don't know how to deduce $H$ from "clues" efficiently ☹.

[Ettinger-Høyer-Knill '04]: [Departed from QFT methodology.]

- We can create samples of the mystery mixed state $\rho_H$.
- We know $\rho_H$ is one of $\{\rho_{H_1}, \rho_{H_2}, \ldots \rho_{H_m}\}$, where $H_1, \ldots, H_m$ are all subgroups of $G$ ($m \leq |G|^{\log |G|}$)
- How many samples needed to identify $H$ ... info-theoretically? Algorithmically efficiently?

Like a classical statistics/learning problem: "Hypothesis Testing".

Compare: Given samples from mystery prob dist. $p \in \{p_1, \ldots, p_m\}$ how many samples needed to identify $p$ whp?

Answer: if $p_i$'s "sufficiently different", $\approx \log m$ suffice, info-theoretically.

Quantumly: can show the same!

[Need a quantum notion of $p_i$'s being "sufficiently distinct, plus some understanding of "quantum probability/stats/info theory, which we'll develop! ]

$\Rightarrow \log(|G|^{\log|G|}) = \log^2|G| = (\log N)^2 \approx n^2$ samples — applications of QF — suffice to solve $HSP_G$ ... info-theoretically.... ☹