Part II:

The Abelian Hidden Subgroup Problem is a Holy Grail

Def: A group is a pair $(G, \cdot)$, where

(a) G is a non-empty set,

(b) $\cdot : G \times G \to G$,

such that:

(i) $\forall a, b, c \in G$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$ (associativity)

(ii) $\exists e \in G$ s.t. $\forall a \in G$,

$$a \cdot e = e \cdot a = a$$ ($\exists$ identity)

(iii) $\forall a \in G$, $\exists b \in G$ s.t.

$$a \cdot b = b \cdot a = e.$$ ($\exists$ inverses)

Ex:

- $(\mathbb{Z}, +)$
- $(k\mathbb{Z}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{R} \setminus \{0\}, \times)$
- $\mathbb{Z}_n := (\{0, 1, \dots, n-1\}, + \pmod n)$
- $(\mathbb{Z}/n\mathbb{Z})^\times := (\{0, 1, \dots, n-1\}, \times \pmod n)$

Quiz: Is $(\mathbb{Z}, \times)$ a group?

Def: A group $(G, \cdot)$ is abelian iff $\forall a, b \in G$,

$$a \cdot b = b \cdot a \quad \text{(commutativity)}.$$

Quiz: Which of the following groups are abelian?

1. $(\mathbb{Z}, +)$
2. $(k\mathbb{Z}, +)$
3. $(\mathbb{R}, +)$
4. $(\mathbb{R} \setminus \{0\}, \times)$
5. $\mathbb{Z}_n := (\{0, 1, \dots, n-1\}, + \pmod n)$
6. $(\mathbb{Z}/n\mathbb{Z})^\times := (\{0, 1, \dots, n-1\}, \times \pmod n)$

Def: Let $(G, \cdot)$ be a group and $H \subseteq G$ a subset. We call $(H, \cdot)$ a subgroup of G, written

$$H \leq G,$$

iff $(H, \cdot)$ is a group.

Quiz: Which is true, which is false, and why?

1. $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
2. $(\mathbb{Z}, +) \leq (k\mathbb{Z}, +)$, $k \neq 1$

Def: Let $H \leq G$ for some group $(G, \cdot)$. The left cosets of H in G are the sets

$$gH := \{gh \mid h \in H\} \text{ for } g \in G.$$

The right cosets of H in G are the sets

$$Hg := \{hg \mid h \in H\} \text{ for } g \in G.$$

Quiz: For which groups $(G, \cdot)$ is it guaranteed that $\forall g \in G$,

$$gH = Hg$$

i.e., that

left cosets = right cosets?

Def: Let $(G, \cdot)$ be a group. A set $A \subseteq G$ *generates* G iff $\forall g \in G$,
$\exists a_1, \ldots, a_\ell \in A$ s.t.

$$g = a_1 \cdot a_2 \cdot \cdots \cdot a_\ell .$$

A is called a *generating set*.

Quiz: Give a generating set for $(\mathbb{Z}, +)$.

Def: Let $(G, \cdot)$ be a group, $H \leq G$, and X a set. A function

$$f : G \longrightarrow X$$

hides H iff $\forall g_1, g_2 \in G$,

$$f(g_1) = f(g_2) \iff g_1 H = g_2 H.$$

$$\iff$$

"f is constant on the cosets of H, but different on different cosets of H."

Ex:

bit-wise addition Mod 2

- Group $= (\{0,1\}^n, \oplus)$
- $f: \{0,1\}^n \to \{0,1\}$ s.t. $f \equiv 0$.
- Then, f hides $(\{0,1\}^n, \oplus) \leq (\{0,1\}^n, \oplus)$.

Quiz: Why?

Claim: Suppose $f: G \to X$ hides $H \leq G$. Then, by querying f, you can determine H.

Proof: Consider truth table of f:

	g_1	g_2	g_3	g_4	$\cdots$	g_ℓ	$\cdots$	$g_{\lvert G\rvert}$
x_1	•			•		•		
x_2			•					
x_3		•						
$\vdots$								
$x_{\lvert X\rvert}$								•

Then, if g_1, g_4, g_ℓ only elements s.t.

$$f(g_1) = f(g_4) = f(g_\ell) \implies g_1 H = \{g_1, g_4, g_\ell\}$$

So,

$$H = g_1^{-1}(g_1 H).$$

The Hidden Subgroup Problem

Input: A group $(G, \cdot)$, a finite set X, and a function f (for which you have an oracle) that hides some $H \leq G$.

Output: A generating set for H.

Notation:

- $HSP(G, X, f)$ for this problem.
- $AHSP(G, X, f)$ if G is abelian.

Query Complexity

- Naively, both $HSP(G, X, f)$ and $AHSP(G, X, f)$ require $O(|G|)$ queries.
- However, $\exists$ quantum algorithm that solves $AHSP(G, X, f)$ using $O(\log |G|)$ queries!
- Quantum <u>exponential</u> speedup!

Def: A computational problem Γ Karp reduces to a problem Λ, written

$$\Gamma \leq_p \Lambda,$$

iff $\exists$ a poly-time algorithm A that turns instances of Γ into instances of Λ.

Ex:
- Subset Sum $\leq_p$ K-SAT
- Factoring $\leq_p$ K-SAT

Claim: If $\Gamma \leq_p \Lambda$, then a poly-time alg. for Λ implies a poly-time alg. for Γ.

Quiz: Why?

Central Claim:

The AHSP is a Holy Grail because:

- Deutsch-Jozsa $\leq_p$ AHSP(G_1, X_1, f_1)
- Simon's Problem $\leq_p$ AHSP (G_2, X_2, f_2)
- Period Finding $\leq_p$ AHSP (G_3, X_3, f_3)
- Factoring $\leq_p$ AHSP (G_4, X_4, f_4)
- Discrete Log $\leq_p$ AHSP (G_5, X_5, f_5)

for appropriate choices of the groups $G_1, \ldots, G_5$, the sets $X_1, \ldots, X_5$, and the functions $f_1, \ldots, f_5$.

Simon's Problem:

Given oracle access to $f: \{0,1\}^n \to \{0,1\}$ such that

$$f(x) = f(y) \iff x \oplus y \in \{0, s\},$$

recover s.

Claim: Simon's Problem $\leq_p$ AHSP$((\{0,1\}^n, \oplus), \{0,1\}, f)$

Proof:

- $\{s\}$ generates $\{0, s\} \leq (\{0,1\}^n, \oplus)$.
- To see that f hides $\{0, s\}$, note, $\forall g \in \{0,1\}^n$,

$$g\{0, s\} = \{g \oplus 0, g \oplus s\} = \{g, g \oplus s\}.$$

But

$$g \oplus (g \oplus s) = s \implies f(g) = f(g \oplus s).$$

I.e., f is constant on the cosets of $\{0, s\}$.

- Similarly, f is different on different cosets.

QED.

Moral: Quantum computers can efficiently solve the AHSP, and hence can efficiently solve the

- Deutsch-Jozsa Problem
- Simon's Problem
- Period Finding Problem
- Factoring Problem
- Discrete Log Problem

Q: Why "abelian"?

A: The Fourier transform over abelian groups is considerably nicer!

→ look up "Pontryagin duality" to learn more.

Final Remarks:

symmetric group

- Graph Isomorphism $\leq_p$ HSP(S_n, X_1, f_1)
- Shortest Vector Problem $\leq_p$ HSP(D_n, X_2, f_2)

Dihedral group

- Post-quantum cryptosystems rely on assumption that quantum computers cannot solve general HSP!

Thank You!