CS6846 – Quantum Algorithms and Cryptography

Hidden Subgroup Problem

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Goal:

Bernstein Vazirani : $F : \{0,1\}^n \to \{0,1\}$

$F(x) = \langle x, s \rangle \bmod 2$

↳ secret s.

Want s.

Simon's : $F : \{0,1\}^N \to \{0,1\}^N$

L periodic

$F(x) = F(x \oplus L)$ o.w. distinct

Goal: Find L.

Period Finding: $F : Z_N \to Z_N$

$F(x) = F(x+L) = F(x+2L) \cdots$ Goal: Find L.

Think of range as colours.

Quantum Algo:

1) Prepare superposition of inputs.
2) Apply f.
3) Measure function register
   get single random colour.
4) Apply QFT
5) Measure & get clues.

6) Use clues to find solution.

Hidden Subgp Problem.

Example: $\mathbb{Z}_{24} = \{0, 1, \ldots, 23\}$

Operation: $+ \bmod 24$.

Let $H = \{0, 4, 8, 12 \ldots 20\}$

Cosets of H:

$1 + H = \{1, 5, 9 \ldots, 21\}$

$2 + H = \{2, 6, 10 \ldots\}$

$3 + H = \{3, 7 \ldots\}$.

Problem: Given $F: \mathbb{Z}_{24} \to$ Colours, "H periodic"
Find H.

Is HSP solvable efficiently using quantum?

Yes, if group is commutative

↳ Simon's
Bernstein-Vazirani
Shors

Don't know otherwise.

non-commutative

↳ Lattice Problems
(Shortest vector Problem)

Graph Isomorphism

Finite Group: A set G with a binary operation $\circ : G \times G \to G$ s.t.

1) Associativity $(x \circ (y \circ z))$ makes sense

2. Identity e

$$e \circ x = x \circ e = x$$

3. Inverse : $\forall \; x \in G, \; \exists \; x' \in G$

s.t $x \circ x' = x' \circ x = e$.

Subgroup: subset which is also a group.

Non-Commutative Groups:

- Symmetric group S_n.

G: set of all permutations π

where $\pi : \{1, 2 .. n\} \to \{1, 2, .., n\}$.

group operation: composition.

$1 \to 2$
$2 \to 1$
$3 \to 3$
π_1

$1 \to 2$
$2 \to 3$
$3 \to 1$
π_2

$\pi_1 \circ \pi_2 \neq \pi_2 \circ \pi_1$

Identity? Identity permutation.

Inverse ✓. Associativity ✓.

Dihedral Group:

G_N: permutations $\pi : \{1, 2 \ldots N\} \to \{1, 2, \ldots N\}$ that are "self isomorphisms" of an N cycle graph.

$N-1$ non-trivial rotations

N reflections

D_N is a subgroup of S_N generated by

a rotation $1 \to 2,\ 2 \to 3,\ \ldots\ n \to 1$

& reflection $1 \to n,\ n \to 1$

$2 \to n-1,\ n-1 \to 2$ and so on

Coset of H is denoted by xoH.

- $|xH| = |H| \quad \forall\ x \in G$
- cosets of H partition G.

Let $F: G \to$ colours, F is H-periodic if
- for each coset $x \circ H$, F has the same colour on all elements
- F gives different colours to different cosets.

Simons: $G = F_2^n$.

$H = \{0, l\}$

Cosets: $\{x, x \oplus l\}$.

Bernstein-Vazirani :

$G = F_2^n$

$H = \{x : \langle x, s \rangle = 0 \bmod 2\}$

only one other coset

$\{x : \langle x, s \rangle = 1 \bmod 2\}$.

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

H is generated by L

$\{0, L, 2L \ldots\}$

Cosets translates $\{x + L, x + 2L \ldots\}$.