The Hidden Subgroup Problem

Ketan Patel

May 13, 2002

Outline

- Preliminaries
- Simon’s Problem
- Integer Factoring / Order Finding
- Hidden Subgroup Problem
- Generalized Fourier Transform
- Non-Abelian Groups

Groups

- Group \((G, +)\): closure, associativity, identity, inverses
- Abelian Group: group satisfying commutativity
- Subgroup \(K\) of \(G\): subset of \(G\) forming a group
- Coset of \(K\): translation of a subgroup \(K\)

Examples of groups:
- \((\mathbb{Z}_n, +)\) additive group of integers mod \(n\)
- \((\mathbb{R}, \ast)\) multiplicative group of nonzero real numbers
- \((\mathbb{B}^n, +)\) additive group of binary \(n\)-tuples \((\equiv\) bitwise \(\oplus)\)
- \((S_n, \ast)\) group of permutations on \(n\) elements \((\ast \equiv\) composition)
Quantum Fourier Transform

$n$-qubit Quantum Fourier Transform ($N = 2^n$)

$$ |x⟩ \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp^{2\pi i xk/N} |k⟩ $$

Simon's Problem

Given: function $f : B^n \rightarrow B^n$

$$ f(x) = f(y) \quad \text{iff } x \oplus y = \beta \quad \text{for all } x, y \in B^n $$

$f$ has “periodicity” $\beta$

Goal: Determine $\beta$ efficiently

Simon's Algorithm

Step 0) Prepare $2^n$ qubits in $|0⟩$ state

Step 1) Create superposition of all basis states in first $n$ qubits

Step 2) Apply $U_f$

$$ \sum_x |x⟩ |0⟩ \rightarrow \sum_x |x⟩ |f(x)⟩ $$

Step 3) Measure last $n$ qubits

$$ \sum_x |x⟩ |f(x)⟩ \rightarrow (|x_0⟩ + |x_0 \oplus \beta⟩) \otimes |f(x_0)⟩ $$

Measuring 1st $n$ qubits yields no information about $\beta$

Simon's Algorithm (cont.)

Step 4) Apply Hadamard Transform to first $n$ qubits

$$ |x_0⟩ + |x_0 \oplus \beta⟩ \rightarrow \sum_y \left( (-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus \beta) \cdot y} \right) |y⟩ $$

$$ = \sum_{y : y \cdot \beta = 0} (-1)^{x_0 \cdot y} |y⟩ \quad \Leftarrow x_0 \text{ only affects phase} $$

Step 5) Measure first $n$ qubits and get $y_i$ such that $y_i \cdot \beta = 0$

Step 6) Repeat enough times ($O(n^2)$) to get system of equations

$$ \begin{bmatrix} y_0(1) & y_0(2) & \cdots & y_0(n) \\ y_1(1) & y_1(2) & \cdots & y_1(n) \\ \vdots & \vdots & \ddots & \vdots \\ y_k(1) & y_k(2) & \cdots & y_k(n) \end{bmatrix} \begin{bmatrix} \beta(1) \\ \beta(2) \\ \vdots \\ \beta(n) \end{bmatrix} = 0 $$

Step 7) Solve for $\beta$
Integer Factoring

Integer factoring can be mapped to order finding

Problem: Find factor of $N$  ⇒  Problem: Find least integer $r$ such that $y^r \equiv 1 \pmod{N}$

Step 0) Select integer $a < N$ at random
Step 1) Use Euclid’s algorithm to compute $\text{gcd}(a, N)$
Step 2) If $> 1$ done
Step 3) Otherwise use order finding algorithm to find least $r$ for $ar \equiv 1 \pmod{N}$
Step 4) If $r$ is odd or $ar = 2^{-1} \pmod{N}$ start over
Step 5) Calculate $\alpha$ and $\beta$:

$$a^r - 1 = \left(\frac{a^{r/2} - 1}{\alpha}\right) \left(\frac{a^{r/2} + 1}{\beta}\right) \equiv 0 \pmod{N}$$

Step 6) If $N|\alpha$ or $N|\beta$ start over
Step 7) Compute $\text{gcd}(N, \alpha)$ and $\text{gcd}(N, \beta)$

Order Finding Algorithm

Step 0) Prepare $t + \lceil \log_2 N \rceil$ qubits in $|0\rangle$ state (Let $T = 2^t$)
Step 1) Create uniform superposition on first $t$ qubits
Step 2) Apply $U_f$

$$\sum_x |x\rangle \rightarrow \sum_x |x\rangle |y^x \pmod{N}\rangle$$

Step 3) Measure second register

$$\sum_x |x\rangle |y^x\rangle \rightarrow \sum_x |\lambda x^0 + \lambda r\rangle |y^x\rangle$$

Step 4) Apply Discrete Fourier Transform to first register

$$\sum_\lambda |\lambda x_0 + \lambda r\rangle \rightarrow \sum_\lambda \sum_k \exp^{2\pi i (\lambda x_0 + \lambda r)/T} |k\rangle$$

$$= \sum_\lambda \sum_k \exp^{2\pi i \lambda x_0 / T} \sum_k \exp^{2\pi i \lambda r / T}$$

$$\approx \sum_k \exp^{2\pi i k x_0 / r} \left|\frac{kT}{r}\right\rangle$$

Hidden Subgroup Problem

Suppose

- $K$ is a subgroup of a group $G$
- $f : g \rightarrow x$ function from $G$ to discrete set $X$
- $f(g_1) = f(g_2) \Rightarrow g_2 \in g_1 + K$

Problem: Find generating set for $K$

Example (Simon’s Problem): $K = \{0, \beta\}$
More Group Theory

Representation \( \rho(G) \): Mapping from \( G \) to group of complex matrices preserving group properties (homomorphism) e.g. \( \rho(g_i)\rho(g_j) = \rho(g_i + g_j) \)

Irreducible Representation \( \rho \): \( \rho \) cannot be written as \( \rho_1 \otimes \rho_2 \)

Example: The irreducible representations of \( Z_4 \)

\begin{align*}
\rho(0) & \quad \rho(1) & \quad \rho(2) & \quad \rho(3) \\
\rho_1 & \quad 1 & \quad 1 & \quad 1 & \quad 1 \quad \text{trivial representation} \\
\rho_2 & \quad 1 & \quad -i & \quad -1 & \quad i \\
\rho_3 & \quad 1 & \quad -1 & \quad 1 & \quad -1 \\
\rho_4 & \quad 1 & \quad i & \quad -1 & \quad -i
\end{align*}

Character \( \chi(\rho) \): Mapping defined by \( \rho(g_i) \rightarrow \text{trace}(\rho(g_i)) \)

For Abelian groups irr. representations are 1-D \( \Rightarrow \) irreducible \( \chi(\rho) = \rho \).

Fourier Transform over \( G \)

Fourier Transform: Transformation from standard basis of group elements to basis of irreducible characters of \( G \)

Properties:

- subgroup \( K \): \( \chi(k) = 1 \) for all \( k \in K \)
  \[
  K = \bigcap_{\chi \in K^\perp} \ker \chi
  \]

- shift invariance
  \[
  \sum_{k \in K} |g+k \rangle \langle g| = \sum_{\chi \in K^\perp} \chi(g)|\chi\rangle
  \]

General HSP Algorithm

Step 1) Create uniform superposition of states in coset of \( K \)

Step 2) Apply Fourier Transform over \( G \)

Step 3) Sample distribution \( \chi_i \in K^\perp \)

Step 4) Reconstruct (classically) \( K = \cap \ker \chi_i \)

General Issues

- Constructing initial superposition may be nontrivial

- Efficient FT over group may not be known

- Group may not be known (e.g., factoring)
Non-Abelian Groups

Issues for Non-Abelian case:

- Non-unique Fourier Transform
- Efficient implementation of FT
- Determining subgroup from sampling of FT
- In general no shift-invariant basis

Graph Isomorphism

Let $M_A, M_B$ be the incidence matrices of graphs $A$ and $B$

$A \cong B$ if $P(M_A) = M_B$ for some permutation matrix $P$

Problem: Given $A$ and $B$ determine if $A \cong B$

Formulate as Non-abelian HSP:

- Let $C = A \cup B, \quad L_A = \text{vertices of } A$ and $L_B = \text{vertices of } B$
- Automorphism group of $C$, $K$ is a subgroup of $S_{2n}$
- If $A \cong B$ all $k \in K$ will map $L_A \mapsto L_B$
- Otherwise half of $K$ will map $L_A \rightarrow L_B$
- Therefore sampling $K$ will determine if $A \cong B$

Unfortunately generating superposition of elements of $K$ nontrivial

Results for Non-Abelian Case

- Solved for normal subgroup assuming efficient FT (Hallgren et al. 2000)
- Solvable if $\cap$ normalizers of all subgroups is large (Grigni et al. 2000)
- “Solved” for dihedral groups — need exponential post-processing (Ettinger and Høyer 2000)
- Solved for groups formed by certain wreath products (Rötteler & Beth 1998)
- Efficient FT over $S_n$ known (Beals 1997)

References

  quant-ph/0012084
  quant-ph/9707033
  www.cs.caltech.edu/~hallgren/repst1.pdf
- Hallgren - Quantum Fourier Sampling, the Hidden Subgroup Problem, and Beyond (2000)