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:

$(Z_n, +)$ additive group of integers mod n

$(R, *)$ multiplicative group of nonzero real numbers

$(B^n, +)$ additive group of binary n-tuples $(+ \equiv$ bitwise $\oplus)$

$(S_n, *)$ group of permutations on n elements $(* \equiv$ composition$)$

Hadamard Transform

1-qubit Hadamard

$$H\left(\alpha|0\rangle+\beta|1\rangle\right)=\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}+\beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Applying Hadamard to n qubits individually

$$H_n|x\rangle=\frac{1}{\sqrt{2^n}}\sum_y(-1)^{x\cdot y}|y\rangle$$

Note: $H_n|0\rangle$ gives equal superposition of all basis states

Quantum Fourier Transform

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

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

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" β

Goal: Determine β efficiently

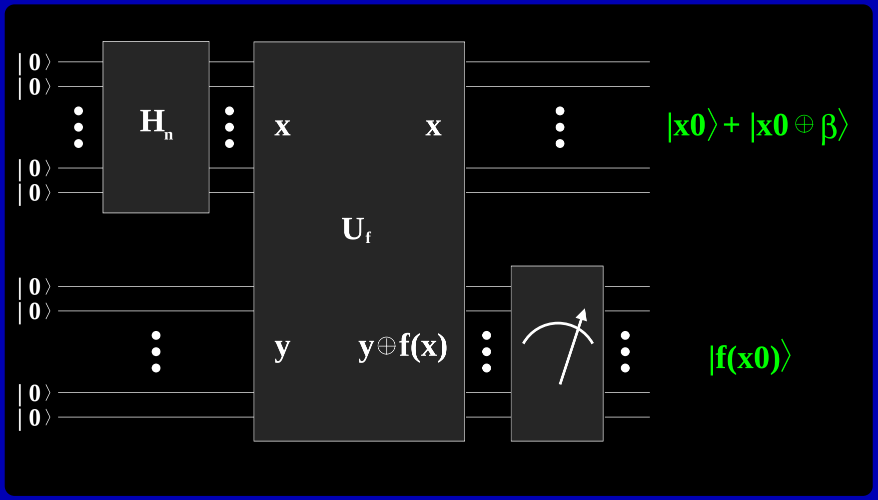
Simon's Algorithm

Step 0) Prepare $2n$ qubits in $|0\rangle$ state

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

Step 2) Apply U_f

$$\sum_x |x\rangle\,|0\rangle \rightarrow \sum_x |x\rangle\,|f(x)\rangle$$



Step 3) Measure last n qubits

$$\sum_x |x\rangle\,|f(x)\rangle \;\rightarrow\; \underbrace{(|x_0\rangle + |x_0 \oplus \beta\rangle)}_{\text{state of 1st n qubits}} \;\otimes\; |f(x_0)\rangle$$

Measuring 1st n qubits yields no information about β

Simon's Algorithm (cont.)

Step 4) Apply Hadamard Transform to first n qubits

$$
\begin{aligned}
|x_0\rangle + |x_0 \oplus \beta\rangle &\rightarrow \sum_y \left((-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus \beta) \cdot y} \right) |y\rangle \\
&= \sum_{y:\ y \cdot \beta = 0} (-1)^{x_0 \cdot y} |y\rangle
\end{aligned}
$$

$\Leftarrow x_0$ 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

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

Step 7) Solve for β

Integer Factoring

Integer factoring can be mapped to order finding

Problem: Find factor of N $\Rightarrow$ Problem: Find least integer r such that $y^r \equiv 1 (\text{mod } N)$

Step 0) Select integer $a < N$ at random
Step 1) Use Euclid's algorithm to compute $\gcd(a, N)$
Step 2) If > 1 done
Step 3) Otherwise use order finding algorithm to find least r for

$$a^r \equiv 1 \ (\text{mod } N)$$

Step 4) If r is odd or $a^{r/2} \equiv -1$ (mod N) start over
Step 5) Calculate α and β:

$$a^r - 1 = \underbrace{\left(a^{r/2} - 1\right)}_{\alpha} \underbrace{\left(a^{r/2} + 1\right)}_{\beta} \equiv 0 \ (\text{mod } N)$$

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

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

$$\sum_x |x\rangle\,|0\rangle \rightarrow \sum_x |x\rangle\,|y^x \text{ mod } N\rangle$$

Step 3) Measure second register

$$\sum_x |x\rangle\,|y^x\rangle \rightarrow \sum_\lambda |x_0+\lambda r\rangle\,|y^{x_0}\rangle$$

Step 4) Apply Discrete Fourier Transform to first register

$$\begin{aligned}
\sum_\lambda |x_0+\lambda r\rangle \quad &\rightarrow \quad \sum_l \sum_\lambda \exp^{2\pi i l (x_0+\lambda r)/T}\,|l\rangle \\
&= \quad \sum_l \exp^{2\pi i l x_0/T}\,|l\rangle \overbrace{\sum_\lambda \exp^{2\pi i l \lambda r/T}}^{\approx 0 \text{ if } lr\neq kT} \\
&\approx \quad \sum_k \exp^{2\pi i k x_0/r}\left|\frac{kT}{r}\right\rangle
\end{aligned}$$

Order Finding Algorithm (cont.)

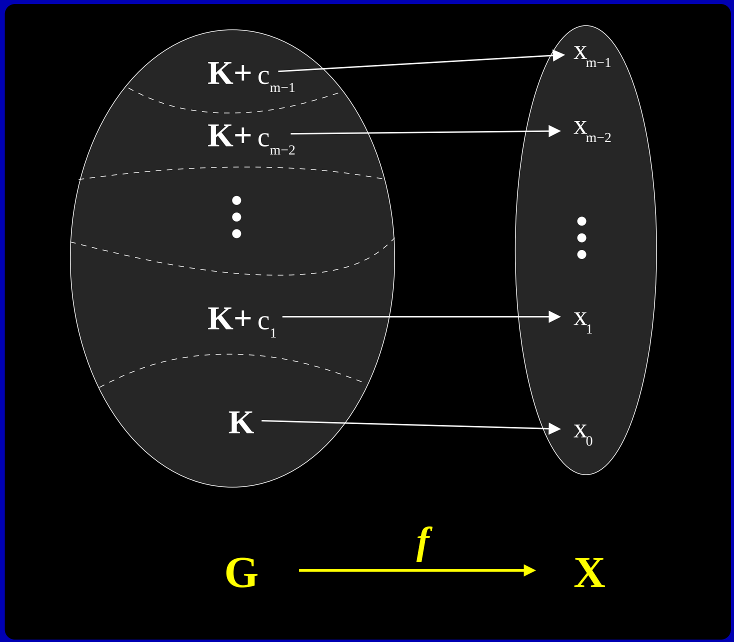
Step 5) Measure first register and get $c = k(T/r)$

Step 6) Use continued fraction algorithm to retrieve r

Hidden Subgroup Problem

Suppose

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



Problem: Find generating set for K

Example (Simon's Problem): $K = \{0, \beta\}$

More Group Theory

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

Irreducible Representation ρ: ρ cannot be written as $\rho_1 \oplus \rho_2$

Example: The irreducible representations of Z_4

	$\rho(0)$	$\rho(1)$	$\rho(2)$	$\rho(3)$	
ρ_1	1	1	1	1	$\Leftarrow$ trivial representation
ρ_2	1	$-i$	-1	i	
ρ_3	1	-1	1	-1	
ρ_4	1	i	-1	$-i$	

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

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 $K \stackrel{FT}{\rightarrow} K^{\perp} := \{\chi : \chi(k) = 1 \quad \text{for all } k \in K\}$

$$K = \bigcap_{\chi \in K^{\perp}} \ker \chi$$

- shift invariance

$$\sum_{k \in K} |g+k\rangle \stackrel{FT}{\rightarrow} = \sum_{\chi \in K^{\perp}} \chi(g) |\chi\rangle$$

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

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

Formulate as Non-abelian HSP:

- Let $C = A \cup B$, $L_A = \{\text{vertices of } A\}$ and $L_B = \{\text{vertices of } B\}$
- Automorphism group of C, K is a subgroup of S_{2n}
- If $A \not\simeq B$ all $k \in K$ will map $L_A \xrightarrow{k} L_A$
  otherwise half of K will map $L_A \longrightarrow L_B$
- Therefore sampling K will determine if $A \simeq B$

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

- Jozsa - Quantum Factoring, Discrete Logarithms, and the Hidden Subgroup Problem (2000)
  quant-ph/0012084

- Jozsa - Quantum Algorithms and the Fourier Transform (1997)
  quant-ph/9707033

- Hallgren & Russell - The Hidden Subgroup Problem and Quantum Computation Using Group Representations (2001)
  www.cs.caltech.edu/ hallgren/reps1.pdf

- Hallgren - Quantum Fourier Sampling, the Hidden Subgroup Problem, and Beyond (2000)
  www.cs.caltech.edu/ hallgren/thesis.pdf