CS-405
Quantum Computation

Group members:

- Trusha Sanghvi 202001188
- Chaitri Gudkha 202003022
- Nikhil Vaghasiya 202003042

The Hidden Subgroup Problem

Let G be a group and H $\subseteq$ G one of its subgroup. Let S be any set and f : G $\rightarrow$ S a function that distinguishes cosets of H i.e. $\forall\ g_1, g_2 \in G$, $f(g_1) = f(g_2) \Leftrightarrow g_1H = g_1 H$. The hidden subgroup problem (HSP) is to determine the subgroup H using calls to f

An algorithm for the hidden subgroup problem is said to be efficient iff it returns a generating set of elements of H using a complexity polynomial in $n = \lceil \log |G| \rceil$.

Examples:

- ➢ Simon's Problem
- ➢ Shor's Algorithm (order finding subroutine)
- ➢ Discrete logarithm

Examples

Discrete logarithm

$a, b \in G'$, find t s.t. $b = a^t$

Simon's Problem

Given f then $f(x) = f(x')$ iff $x = x' \oplus s$, so find s

Shor's Factoring

Given $x \in Z_n^*$ find order of x

Discrete logarithm

- Let a, b $\in Z_N^*$ ($N \in Z \geq 2$) such that $b = a^t$ mod N. Find t.
- The algorithm for discrete log problem is based on phase estimation

Discrete logarithm

- We first find r (order of a mod N) using Shor's algorithm in polynomial time.
- By the principle of group theory we know that $t \in Z_r$. Let $n = \lfloor \log_2(r + 1) \rfloor$.
- Let $m = \lfloor \log_2(N + 1) \rfloor$, i.e., m is the minimum number of bits needed to represent N in binary. Now, for $a \in Z_N^*$, define Ua as follows:

$$U_a |x\rangle = |a*x \bmod N\rangle \text{ where } x \in Z_N^*$$

- To implement U_a as a quantum circuit, we have to first make it into a unitary operator. Doing so may require some auxiliary qubits.
- Consider the following vectors for $k \in Z_r$:

$$|u_k\rangle = \sum_{j=0}^{r-1} \omega_r^{-jk} |a^j \bmod N\rangle / r^{1/2} \text{ where } \omega_r := e^{2\pi i/r}.$$

- $|u_k\rangle$ is eigenvector of U_a i.e., $U_a|u_k\rangle = \omega_r |u_k\rangle$ and

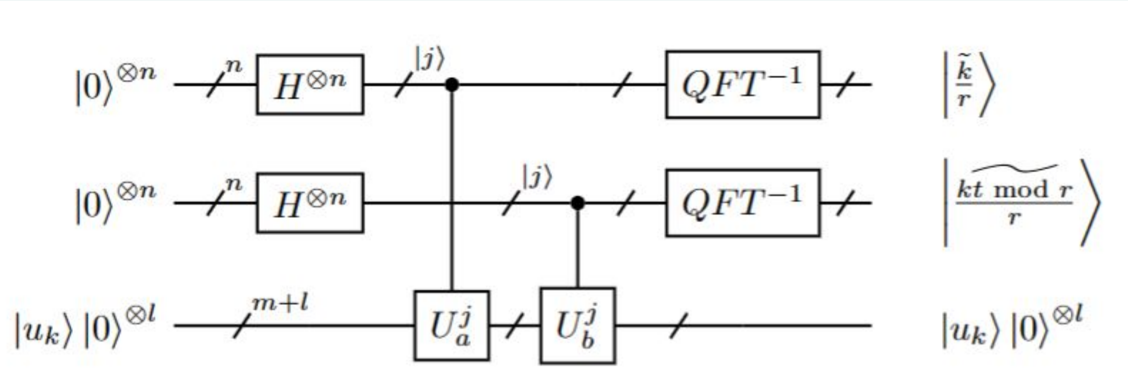
$$\sum_{k=0}^{r-1} |u_k\rangle / r^{1/2} = |1\rangle \qquad \text{A}$$

Discrete logarithm

- Since, $b = a^t \bmod N$, $U_b = U_a^{\,t}$. So, for $k \in Z_r$,

$$U_b\,|u_k\rangle = U_a^{\,t}\,|u_k\rangle = \omega_r^{\,kt \bmod r}\,|u_k\rangle$$

- Phase estimation circuit for DLP:



Discrete logarithm

- The circuit can be thought of as consisting of two phase estimation circuits. The details of the implementation of the Controlled-U_a circuit in O(poly(n)) gates. Since U_a and U_b share eigenvectors, the lower parts of the phase estimation circuit can be put in succession(i.e. In series). So, for $k \in Z_r$, the circuit implements that following transformation:

$$|0\rangle^{\otimes n} |0\rangle^{\otimes n} |u_k\rangle |0\rangle^{\otimes l} \mapsto |k'/r\rangle |(k't \bmod r)/r\rangle |u_k\rangle |0\rangle^{\otimes l}$$

- Instead of a particular eigenvector $|u_k\rangle$, if we input $|1\rangle$, then according to equation (A), we will get:

$$\sum_{k=0}^{r-1} |k'/r\rangle |(k't \bmod r)/r\rangle |u_k\rangle |0\rangle^{\otimes l} / r^{1/2}$$

Discrete logarithm

- So, by measuring the first two registers, we can find k/r and $(kt \bmod r)/r$ where each $k \in Z_r$ occurs with probability $1/r$. Since we know r, we can find k and $kt \bmod r$. Repeat the algorithm sufficient number of times to find $k_1, k_2 \in Z_r$ such that $\gcd(k_1, k_2) = 1$.
- Let $v_1 = k_1 t \bmod r$ and $v_2 = k_2 t \bmod r$. Since $\gcd(k_1, k_2) = 1$, there exist $\lambda_1, \lambda_2 \in Z$ such that $\lambda_1 k_1 + \lambda_2 k_2 = 1$. Since $t \in Z_r$,

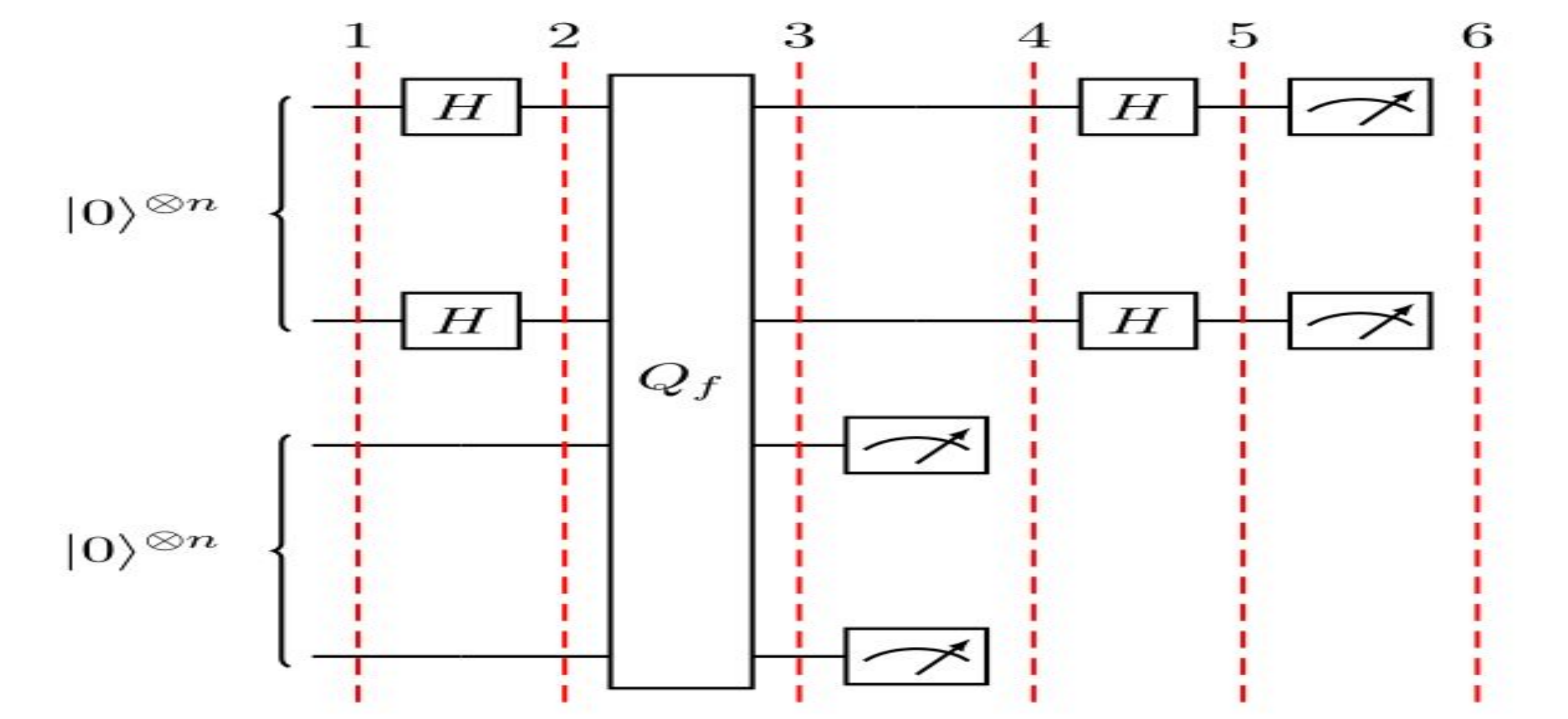
$$\begin{aligned} t &= t \bmod r, \\ &= (\lambda_1 k_1 + \lambda_2 k_2)*t \bmod r \\ &= (\lambda_1 k_1 + \lambda_2 k_2) \bmod r \\ &= (\lambda_1 v_1 + \lambda_2 v_2) \bmod r \end{aligned}$$

- So puting value of λ_1 , λ_2 , v_1 and v_2 we get t.

Simon's Problem

- Given a blackbox implementation of a function $f : \{0, 1\}^n \rightarrow X$ for some set X.
- Where $f(x) = f(y)$ if and only if $x \oplus a = y$ for some unknown $a \in \{0, 1\}^n$.

Circuit for Simon's Problem



Circuit for Simon’s Problem

The algorithm involves the following steps,

Two -qubit input registers are initialized to the zero state:

$$|\psi_1\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n}$$

Apply a Hadamard transform to the first register:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle^{\otimes n}$$

Apply the query function

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$

Circuit for Simon's Problem

Measure the second register. A certain value of will be observed. Because of the setting of the problem, the observed value could correspond to two possible inputs: and . Therefore the first register becomes:

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$$

where we omitted the second register since it has been measured.

Apply Hadamard on the first register:

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{z\in\{0,1\}^n} [(-1)^{x\cdot z} + (-1)^{y\cdot z}]|z\rangle$$

Circuit for Simon’s Problem

Measuring the first register will give an output only if:

$$(-1)^{x.z} = (-1)^{y.z}$$

which means:

$$\begin{aligned} x \cdot z &= y \cdot z \\ x \cdot z &= (x \oplus b) \cdot z \\ x \cdot z &= x \cdot z \oplus b \cdot z \\ b \cdot z &= 0 \pmod 2 \end{aligned}$$

A string will be measured, whose inner product with . Thus, repeating the algorithm times, we will be able to obtain different values of and the following system of equation can be written:

$$\begin{cases} b \cdot z_1 = 0 \\ b \cdot z_2 = 0 \\ \quad \vdots \\ b \cdot z_n = 0 \end{cases}$$

Circuit for Simon's Problem

- From which b can be determined, for example by Gaussian elimination(n^3).

- Here we can observe that number of queries in classical algorithm is about $2^{n-1} + 1$ and our quantum solution requires O(n) queries.