COL7160 : Quantum Computing

Lecture 17: Solving the Hidden Subgroup Problem

Instructor: Rajendra Kumar **Scribe:** Harshal Singh Sindal

1 Recap: Discrete Logarithm Reduction

Setup. Given a generator $g \in G$ and $h \in G$ such that $h = g^x$.
Goal. Find x.

Assume $|G| = N$, hence $g^N = e$ where e is the identity element in G.
Define the function

$$f : \mathbb{Z}_N \times \mathbb{Z}_N \longrightarrow G, \qquad f(a,b) = g^a h^{-b}.$$

Then

$$f(a,b) = f(a',b') \iff g^a h^{-b} = g^{a'} h^{-b'} \iff a - xb = a' - xb',$$

since g is a generator. This is equivalent to $a - a' = x(b - b')$.

Consider the group

$$H = \{(0,0),\ (x,1),\ (2x,2),\ \ldots\} \subset \mathbb{Z}_N \times \mathbb{Z}_N$$

under addition modulo N. Note that the generator of H is $\langle (x,1) \rangle$.
This is an instance of the **Hidden Subgroup Problem**, where H is the hidden subgroup in G under the function f.

2 Solving the Hidden Subgroup Problem

The quantum algorithm to solve the hidden subgroup problem instance encountered above is as follows:

1. Start with quantum state $|0^n, 0^n, 0^n\rangle$, where $n = \log_2 N$. Convert to $\sum_{a,b \in \mathbb{Z}_N} |a, b, 0^n\rangle$. Note that we have seen this conversion when N is a power of 2 (Using Hadamard Gate). For now we assume that this conversion is possible for general N.

2. Apply oracle U_f to get $\sum_{a,b \in \mathbb{Z}_N} |a, b, f(a,b)\rangle$.

3. Measure the third register to collapse the state to

$$\sum_{\substack{a,b \in \mathbb{Z}_N \\ a - bx \equiv \delta \bmod N}} c.\, |a, b, g^\delta\rangle = \sum_{b \in \mathbb{Z}_N} c.\, |\delta + bx, b, g^\delta\rangle$$

   where $\delta \in N$ and c is the normalization factor.

4. Apply Quantum Fourier Transform ($\text{QFT}_N \otimes \text{QFT}_N$) on the first two registers to get

$$\begin{aligned}
&c. \sum_{b \in \mathbb{Z}_N} \left(\sum_{k_1 \in \mathbb{Z}_N} \omega_N^{k_1 \cdot (\delta + bx)} |k_1\rangle \right) \otimes \left(\sum_{k_2 \in \mathbb{Z}_N} \omega_N^{b \cdot k_2} |k_2\rangle \right) \otimes |g^\delta\rangle \\
&= c. \sum_{b \in \mathbb{Z}_N} \sum_{k_1, k_2 \in \mathbb{Z}_N} \omega_N^{k_1(\delta + bx) + k_2 b} |k_1, k_2\rangle \otimes |g^\delta\rangle \\
&= c. \sum_{k_1, k_2 \in \mathbb{Z}_N} \sum_{b \in \mathbb{Z}_N} \omega_N^{k_1(\delta + bx) + k_2 b} |k_1, k_2\rangle \otimes |g^\delta\rangle \;=\; c. \sum_{k_1, k_2 \in \mathbb{Z}_N} \omega_N^{k_1 \delta} \sum_{b \in \mathbb{Z}_N} \omega_N^{b(k_1 x + k_2)} |k_1, k_2\rangle \otimes |g^\delta\rangle .
\end{aligned}$$

   Note that the dimension of Fourier Transform used here need not be a power of 2 as done in class.

5. For any state $|k_1, k_2\rangle$, the amplitude is nonzero if and only if

$$k_1 x + k_2 \equiv 0 \bmod N.$$

The resulting state is a uniform distribution over all such states corresponding to admissible pairs of k_1 and k_2.

To find x, we run the algorithm multiple times to sample multiple pairs (k_1, k_2). Once we have two pairs such that $\gcd(k_1, k_1') = 1$, then x can be found.

The above algorithm needs to address two problems, stemming from N not being a power of 2, as in steps 1 and 4. For step 1, we can define a membership function $g : \{0,1\}^{\lceil \log_2 N \rceil} \to \{0,1\}$ where $g(x) = 1$ iff $x < N$. We can then keep an ancilla qubit and use the oracle of this function, and then measure this qubit. We proceed with the algorithm only when the ancilla collapses to $|1\rangle$.
The algorithm also requires the Fourier transform on N dimensions, which can be any integer. We have only seen an efficient circuit for the QFT when N is a power of 2. In this case, we will apply the QFT over N', which is the smallest power of 2 greater than N. This will change our calculations, but the same idea will still work to find x.

The above algorithm holds only for Abelian Groups. We don't know yet how to extend to non Abelian groups. But even for Abelian groups, the group can be totally arbitrary. How can we use the above algorithm for such groups?

Theorem 1 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite abelian group is isomorphic to a direct product of cyclic groups:*

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}.$$

Using such a homomorphism, we can extend our algorithm to general finite Abelian groups.

3 Graph Isomorphism

Definition 2. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are *isomorphic* if there exists a permutation $\pi : [n] \to [n]$ such that

$$(i,j) \in E_1 \iff (\pi(i), \pi(j)) \in E_2.$$

No efficient classical algorithms are known for solving this problem. However, it can be reduced to a Hidden Subgroup Problem instance, on the *symmetric group*:

$$S_n = \{\text{all permutations of } \{1, \ldots, n\}\}, \qquad |S_n| = n!$$

and the operation is composition of permutations.
The catch here is that the group is not Abelian, and no Quantum Algorithm is known to solve it efficiently.
Exercise: Identify the subgroup in the above reduced HSP instance.

4 Learning with Errors (LWE)

The popular Learning With Errors (LWE) problem finds its applications in developing post-quantum cryptosystem.

Definition 3 (Learning with Errors)**.** Let $A \leftarrow \mathbb{Z}_q^{n \times m}$, let e be a *small-length* error vector in $\mathbb{Z}_q^m$, and let $s \in \mathbb{Z}_q^n$. Given $(A,\ s^\top A + e)$, find s.

Dihedral Group

The *dihedral group* D_N is the symmetry group of a regular N-gon:

$$D_N = \{(s^a, r^b)\}, a \in \mathbb{Z}_N, b \in \mathbb{Z}_2$$

where s denotes rotation and r denotes reflection.
Some of the subgroups of D_N are:

$$\langle (x,0) \rangle, \quad \langle (y,1) \rangle, \quad \langle (x,0),\ (y,1) \rangle.$$

Exercise: Solve the dihedral subgroup problem when hidden subgroup H is of form $\langle (x,0) \rangle$.

Theorem 4 ([Reg04, BKSW18])**.** *A polynomial-time quantum algorithm for the dihedral hidden subgroup problem gives a polynomial-time quantum algorithm for LWE.*

References

[BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen. Learning with errors and extrapolated dihedral cosets. In *IACR international workshop on public key cryptography*, pages 702–727. Springer, 2018.

[Reg04] Oded Regev. Quantum computation and lattice problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.