COL7160 : Quantum Computing

Lecture 16: Hidden Subgroup Problem

Instructor: Rajendra Kumar

Scribe: Daksh Kansil

1 Introduction

The hidden subgroup problem is one of the central problems in quantum computing, since several important quantum algorithms can be formulated as special cases of it. Broadly speaking, the problem asks us to determine a subgroup hidden inside a larger group through the behavior of a function that is constant on cosets of that subgroup and distinct across different cosets. This viewpoint provides a common algebraic framework for understanding problems such as Simon's problem, period finding, and the discrete logarithm problem.
To study the hidden subgroup problem, we first need some basic group-theoretic ideas, especially the notion of cosets and how they partition a group. These concepts allow us to precisely describe what it means for a function to "hide" a subgroup and why recovering that subgroup is the main computational task.

2 Theory of Cosets

Let G be a group and let $H \leq G$ be a subgroup. For any $g \in G$, the *left coset* of H corresponding to g is defined as

$$gH = \{gh : h \in H\},$$

and the *right coset* is defined as

$$Hg = \{hg : h \in H\}.$$

Thus, if

$$H = \{h_1, h_2, \ldots, h_k\},$$

then

$$gH = \{gh_1, gh_2, \ldots, gh_k\}, \qquad Hg = \{h_1g, h_2g, \ldots, h_kg\}.$$

We now record some basic properties of cosets.

Lemma 1. *For $g, g' \in G$,*

$$gH = g'H \iff g' \in gH.$$

Proof. First suppose that $gH = g'H$. Since $g' \in g'H$, it follows that $g' \in gH$.
Conversely, suppose $g' \in gH$. Then there exists some $h_0 \in H$ such that

$$g' = gh_0.$$

Hence

$$g'H = (gh_0)H = g(h_0H).$$

Since $h_0 \in H$ and H is a subgroup, we have

$$h_0H = H.$$

Therefore

$$g'H = gH.$$

This proves the result. □

Lemma 2. *Any two left cosets of H are either equal or disjoint.*

Proof. Let gH and $g'H$ be two left cosets. Suppose they are not disjoint. Then there exists some element x such that

$$x \in gH \cap g'H.$$

Since $x \in gH$, we may write

$$x = gh_1$$

for some $h_1 \in H$. Similarly, since $x \in g'H$, we may write

$$x = g'h_2$$

for some $h_2 \in H$.
From $x = gh_1$, we get

$$g = xh_1^{-1}.$$

Substituting $x = g'h_2$, we obtain

$$g = g'h_2h_1^{-1}.$$

Since $h_2h_1^{-1} \in H$, it follows that

$$g \in g'H.$$

By the previous lemma,

$$gH = g'H.$$

Thus, if two cosets intersect, they are equal. Therefore any two cosets are either equal or disjoint. □

Lemma 3. *A left coset gH is a subgroup of G if and only if $g \in H$.*

Proof. If $g \in H$, then

$$gH = H,$$

since multiplying all elements of H by an element of H keeps us inside H. Hence gH is a subgroup.
Conversely, suppose gH is a subgroup of G. Since every subgroup must contain the identity element e, we have

$$e \in gH.$$

So there exists some $h \in H$ such that

$$gh = e.$$

Hence

$$g = h^{-1}.$$

Because H is a subgroup, $h^{-1} \in H$, and therefore $g \in H$. □

Lemma 4. *The left cosets of H partition the group G.*

Proof. We must show two things: every element of G belongs to some left coset of H, and no element belongs to two distinct left cosets.
First, let $g \in G$. Then

$$g \in gH,$$

because the identity element $e \in H$ and

$$g = ge.$$

So every element of G lies in at least one left coset.
Second, by the previous lemma, any two left cosets are either equal or disjoint. Hence no element can belong to two distinct left cosets.
Therefore the collection of left cosets of H partitions G. □

Note. If G is an abelian group, then all elements commute, so for all $g, h \in G$,

$$gh = hg.$$

Hence in an abelian group, left and right cosets coincide:

$$gH = Hg.$$

3 Statement of the Hidden Subgroup Problem

Let G be a group and let

$$f : G \to X$$

be a function such that for some fixed subgroup $H \leq G$,

$$f(g_1) = f(g_2) \iff g_1 \in g_2 H.$$

Equivalently, f is constant on each coset of H, and two elements take the same value if and only if they belong to the same coset.
Goal: Find H.

4 Generating Sets and Size Bound

For an element $g \in G$, the notation

$$\langle g \rangle$$

denotes the subgroup generated by g.
More generally, for elements $g_1, g_2, \ldots, g_k \in G$, the notation

$$\langle g_1, g_2, \ldots, g_k \rangle$$

denotes the subgroup generated by these elements, i.e. the smallest subgroup of G containing all of them.
To understand how large a generating set needs to be, we first show that whenever a genuinely new generator is added, the size of the generated subgroup increases by at least a factor of 2.

Lemma 5. *Let*

$$H_{i-1} = \langle h_1, h_2, \ldots, h_{i-1} \rangle$$

and

$$H_i = \langle h_1, h_2, \ldots, h_{i-1}, h_i \rangle.$$

If $h_i \notin H_{i-1}$, then

$$|H_i| \geq 2|H_{i-1}|.$$

Proof. Since $H_{i-1} \leq H_i$, every element of H_{i-1} lies in H_i.
Now consider the left coset

$$h_i H_{i-1} = \{h_i h : h \in H_{i-1}\}.$$

Because $h_i \notin H_{i-1}$, this coset cannot be equal to H_{i-1}. Indeed, if

$$h_i H_{i-1} = H_{i-1},$$

then by the coset criterion proved earlier, we would have

$$h_i \in H_{i-1},$$

which is a contradiction.
Hence H_{i-1} and $h_i H_{i-1}$ are distinct cosets of H_{i-1}. Since distinct cosets are disjoint, these two sets are disjoint.

Also, both sets are contained in H_i: clearly $H_{i-1} \subseteq H_i$, and if $x \in h_i H_{i-1}$, then

$$x = h_i h$$

for some $h \in H_{i-1}$. Since both h_i and h lie in H_i, it follows that $x \in H_i$.
Therefore H_i contains two disjoint subsets, namely H_{i-1} and $h_i H_{i-1}$, each of size $|H_{i-1}|$. Thus

$$|H_i| \geq |H_{i-1}| + |h_i H_{i-1}| = 2|H_{i-1}|.$$

□

The previous lemma shows that each time we add a generator that was not already generated by the previous ones, the subgroup size at least doubles.

Lemma 6. *Every subgroup of a finite group G has a generating set of size $O(\log N)$, where $N = |G|$.*

Proof. Let $H \leq G$ be a subgroup, and let

$$H = \langle h_1, h_2, \ldots, h_k \rangle$$

be a generating set of minimal size. Since the generating set is minimal, for each $i \geq 1$ we must have

$$h_i \notin \langle h_1, h_2, \ldots, h_{i-1} \rangle.$$

Otherwise, h_i would be redundant, contradicting minimality.
Define

$$H_i = \langle h_1, h_2, \ldots, h_i \rangle \qquad \text{for } i = 1, 2, \ldots, k.$$

Also let

$$H_0 = \{e\},$$

where e is the identity element.
By the previous lemma, for each $i = 1, 2, \ldots, k$,

$$|H_i| \geq 2|H_{i-1}|.$$

Applying this repeatedly gives

$$|H_k| \geq 2^k |H_0|.$$

Since $|H_0| = 1$, this becomes

$$|H_k| \geq 2^k.$$

But $H_k = H$, and since $H \leq G$,

$$|H| \leq |G| = N.$$

Therefore,

$$2^k \leq N.$$

Taking logarithms,

$$k \leq \log_2 N.$$

Thus H has a generating set of size at most $\log_2 N$, which proves that the size of a smallest generating set is $O(\log N)$.
□

Therefore, in a finite group, a subgroup can always be specified using only logarithmically many generators. This is one reason the hidden subgroup problem appears computationally manageable: instead of outputting all elements of the subgroup, it may suffice to recover a small generating set.

5 Applications of the Hidden Subgroup Problem

We now discuss several important quantum computational problems that can be formulated as special cases of the hidden subgroup problem.

5.1 Simon's Problem

Simon's problem is a special case of the hidden subgroup problem.
Consider the group

$$G = (\{0,1\}^n, \oplus),$$

where the group operation is bitwise XOR. Let

$$f : \{0,1\}^n \to \{0,1\}^m$$

be a function such that there exists a hidden string $s \in \{0,1\}^n$ satisfying

$$f(x) = f(y) \iff x \oplus y \in \{0^n, s\}.$$

Define

$$H = \{0^n, s\} = \langle s \rangle.$$

Then the cosets of H are precisely the sets

$$x \oplus H = \{x, x \oplus s\}.$$

Thus two elements $x, y \in \{0,1\}^n$ satisfy

$$f(x) = f(y)$$

if and only if they lie in the same coset of H. Therefore f hides the subgroup H, and Simon's problem is exactly the hidden subgroup problem over the abelian group $(\{0,1\}^n, \oplus)$.

5.2 Period Finding

Another important example is period finding.
Consider a function

$$f : \mathbb{Z} \to X$$

such that there exists a positive integer r for which

$$f(x) = f(y) \iff x - y \in r\mathbb{Z}.$$

Equivalently, f is constant on residue classes modulo r and takes distinct values on distinct residue classes. In particular,

$$f(x + r) = f(x) \qquad \forall x \in \mathbb{Z}.$$

The goal is to determine the smallest positive integer r for which this holds.
This can be viewed as a hidden subgroup problem over the group $(\mathbb{Z}, +)$. The hidden subgroup is

$$H = r\mathbb{Z} = \{kr : k \in \mathbb{Z}\}.$$

The cosets of H are precisely the residue classes modulo r:

$$a + r\mathbb{Z} = \{a + kr : k \in \mathbb{Z}\}.$$

Hence two integers have the same function value if and only if they lie in the same coset of $r\mathbb{Z}$. Therefore period finding is an instance of the hidden subgroup problem.

5.3 Discrete Logarithm Problem

The discrete logarithm problem can also be reduced to the hidden subgroup problem.
Let p be a prime, and let $g \in \mathbb{Z}_p^*$ be a generator of the multiplicative group $\mathbb{Z}_p^*$. Suppose

$$h = g^x$$

for some unknown $x \in \mathbb{Z}_{p-1}$. The goal is to determine x.
Consider the group

$$G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1},$$

and define the function

$$f : G \to \mathbb{Z}_p^*$$

by

$$f(a, b) = h^{-a} g^b.$$

Since $h = g^x$, we obtain

$$f(a, b) = g^{-ax} g^b = g^{\,b-ax}.$$

Now let $(a, b), (a', b') \in G$. Then

$$f(a, b) = f(a', b') \iff g^{\,b-ax} = g^{\,b'-a'x}.$$

Because g is a generator of $\mathbb{Z}_p^*$, equality of powers is equivalent to equality of exponents modulo $p - 1$. Hence

$$f(a, b) = f(a', b') \iff b - ax \equiv b' - a'x \pmod{p-1}.$$

Rearranging, we get

$$b' - b \equiv (a' - a)x \pmod{p-1}.$$

If we write

$$t = a' - a \in \mathbb{Z}_{p-1},$$

then the above relation becomes

$$b' - b \equiv tx \pmod{p-1}.$$

Therefore

$$(a' - a, b' - b) = (t, tx),$$

which shows that

$$(a', b') - (a, b) \in \langle (1, x) \rangle.$$

Conversely, any difference of the form (t, tx) preserves the value of f. Indeed,

$$f(a + t, b + tx) = h^{-(a+t)} g^{\,b+tx} = h^{-a} g^b \cdot h^{-t} g^{tx}.$$

Since $h = g^x$, we have

$$h^{-t} g^{tx} = g^{-tx} g^{tx} = 1,$$

and therefore

$$f(a + t, b + tx) = f(a, b).$$

Thus two pairs in G have the same function value if and only if they lie in the same coset of the subgroup

$$H = \langle (1, x) \rangle = \{(t, tx) : t \in \mathbb{Z}_{p-1}\}.$$

Therefore the discrete logarithm problem can be formulated as an instance of the hidden subgroup problem.

6 Conclusion

We have seen that the hidden subgroup problem provides a unifying framework for several important quantum problems, including Simon's problem, period finding, and the discrete logarithm problem.