CIS 410 Final Report on Hidden Subgroup Problem

Zhimeng Wang, Dongmin Roh, Matthew Jagielski

June 8, 2016

1 Motivation

The hidden subgroup problem (HSP) is an computational algebra problem which has been shown to have a lot of interesting consequences and motivations. For example, the *Shor's quantum algorithm* of factoring integers and solving the discrete logarithm problem can be reduced to solving the HSP on finite abelian groups.

Definition 1. Given a group G, a subgroup $H \leq G$, and a set X, a function $f : G \to X$ **hides** H if $\forall g_1, g_2 \in G, f(g_1) = f(g_2)$ iff $g_1H = g_2H$, that is, g_1, g_2 are in the same coset of H.

Definition 2. Now, the **Hidden Subgroup Problem (HSP)** is a problem with inputs: a group G, a set X, and a function oracle $f : G \to X$ hiding a subgroup H. The function oracle uses $\log(\mid G \mid + \mid X \mid)$ bits. The desired output is a generating set of H.

It is known that there exits a quantum algorithm which solves with certainty a hidden subgroup problem of an arbitrary finite group in a polynomial (in $log|G|$) number of calls to the oracle. In addition, quantum computers have been shown to have very good speedups for some instances of the problem. In fact, because quantum computers can factor integers much faster than classical computers can, quantum computers can solve the HSP on finite abelian groups in polynomial time.

Two unknowns regarding the HSP are whether the symmetric group and the dihedral group have efficient quantum algorithms for solving HSP. If an efficient quantum algorithm were to be found for the symmetric group HSP, we would have an efficient algorithm for *graph isomorphism*, a very important problem in theoretical computer science and for Eugene Luks. A polynomial time dihedral group HSP algorithm would give a polynomial time algorithm for solving the *shortest vector problem on lattices*, a problem which is...(line truncated)...

Our group has some background in abstract algebra and algebraic number theory, so this is an attractive topic for us to explore. Also, one of us is studying the shortest vector problem for his undergraduate thesis, so this is of increased interest.

2 Quantum Complexity Results

We realize that many of the well-known quantum algorithms such as Deutsch, Simon, Order-finding, Integer factorization, etc are instances of the hidden subgroup problem. Using an algorithm similiar to these problems, we'll see that for a finite abelian group we can solve the HSP efficiently.
Although no efficient quantum algorithm for non-abelian groups fulfills polynomial time complexity, the quantum query complexity is polynomial. This is exponentially better than any classical algorithms.

2.1 Quantum Time Complexity of an Abelian Group

We give an outline of the algorithm that solves the HSP for an abelian group G in a polynomial number of operations in $log|G|$. This algorithm solves with bounded error; we can find a subset that generates the hidden subgroup with probability at least $\frac{2}{3}$. It is worth mentioning that for Abelian groups of smooth order[1], this success probability can be improved to one.
Recall that finite Abelian groups are isomorphic to a product of finite cyclic groups of prime power order. This allows us to perform the quantum fourier transfrom of f over G in an efficient way. (Decomposing an arbitrary abelian group is a difficult problem. However, Shor's quantum algorithm for factorizing integers can be applied to decompose an abelian group efficiently)
Suppose that an abelian group G is isomorphic to a product of cyclic groups $\mathbb{Z}_{t_1} \times \mathbb{Z}_{t_2} \times \cdots \times \mathbb{Z}_{t_k}$. Consider applying the operation $F_G = F_{t_1} \otimes F_{t_2} \otimes \cdots \otimes F_{t_k}$, which performs a quantum fourier transform to each ith state, to some element $g \in G$ (Here, $|g\rangle = |g_1\rangle |g_2\rangle \cdots |g_k\rangle$). Then, we attach an ancilla bit and send the state through the black box to obtain

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

We perform a measurement on the second register to get some value $f(g^{'})$. This leaves the first register to be in the state

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} \left| g^{'} + h \right\rangle$$

where H is our hidden subgroup. We apply the operation F_G once again then measure this first register. With certainty we get a uniformly random element of $H^{\perp}$, which is a dual group of H.[2] Thus, repeating these steps about $n = \lceil log|G| \rceil$ many times gives with high probability a set of generators $g^1, \ldots, g^{O(n)}$ of $H^{\perp}$. The linear congruences corresponding to these elements determine H; randomly pick a solution to each linear congruence to get a uniformly random element of H, repeat this $O(n)$ times gives us a set of generators of H with high probabilty.

[1]The order of a group G is smooth if all prime factors are at most $log^c|G|$ for some fixed constant c

[2]The dual is defined as $H^{\perp} = \{g \in G : \chi_g(h) = 1, \forall h \in H\}$ where $\chi_g(h) = \prod_{i=1}^{k} e^{\frac{2\pi i g_i h_i}{t_i}}$

2.2 Quantum Query Complexity of a Finite Group

Our motivation is to find an efficient quantum algorithm which can solve the HSP for any arbitrary finite group G in a polynomial calls to the given oracle. Given r many distinct subgroups of G, we are looking for a generating set for one of the subgroups. We can assume that any algorithms for the HSP always output a subset of a subgroup H; if an algorithm outputs some subset $X \nsubseteq H$, we simply find the intersection of X with H by keeping $x \in X$ only if $f(x) = f(1_G)$.

Let f be a function satisfying the conditions of the HSP. Fix an ordering of the distinct subgroups $H_1, H_2, \ldots, H_r$ such that $|H_i| \geq |H_{i+1}|$ for all $1 \leq i \leq r$.[3] Also let $N = |G|$ and consider $n = log|G|$ to be the input size. [4]

Theorem 3. *There exists a quantum algorithm that solves the HSP for any finite group G in $O(log^4|G|)$ calls to the oracle. The algorithm has exponentially small error probability in $log|G|$.*

The algorithm considers $2 + 2s$ registers, where s is a positive integer chosen to lower the error probability: 1st contains a subgroup index $1 \leq v \leq r$, 2nd contains a counter $1 \leq l \leq r$, remaining $2s$ are pairs of couplets so that in each couplet the first contains an element of G and the second some image of f. We call the first register in a couplet as a "subgroup" register and the second as a "function" register.

We say that a function f is H-*periodic* if f is constant of the left cosets of a subgroup H of G. H being a *hidden subgroup* of f is an instance of f taking distinct values on distinct cosets of H.

A left *translation* of a subgroup H is a subset $T \subseteq G$ such that for any $g \in G$, $g = th$ for some $t \in T$ and $h \in H$.

We define an operator Test so that $\mathsf{Test} = \mathsf{Test_r} \cdot \cdots \cdot \mathsf{Test_2} \cdot \mathsf{Test_1}$, where each unitary operator $\mathsf{Test_i}$ tests whether f is H_i-periodic. Each $\mathsf{Test_i}$ is defined by $\mathsf{Test_i} = Q_i \otimes P_{s,i} + I \otimes P_{s,i}^{\perp}$ where

$$Q_i : \quad \begin{cases} |0\rangle\,|0\rangle & \mapsto \quad |i\rangle\,|1\rangle \\ |v\rangle\,|l\rangle & \mapsto \quad |v\rangle\,|l+1\rangle\,, \qquad \text{if } l > 0 \end{cases} \qquad \text{and } P_{s,i} = \left(\sum_{t \in T_i} |tH_i\rangle \langle tH_i| \otimes I \right)^{\otimes s}$$

Here Q_i acts on the first two registers so that once the second register is increased from 0 to 1, the first register stays the same, and $P_{s,i}$ is the projector of the s couplets. The effect of $\mathsf{Test_i}$ is that Q_i is applied on the first two registers if s subgroup registers are in coset states of H_i.

We create an initial state to be

$$|\Psi_{init}\rangle = |0\rangle\,|0\rangle \otimes \left(\frac{1}{\sqrt{N}} \sum_{g \in G} |g\rangle\,|f(g)\rangle \right)^{\otimes s}$$

by s many query calls.

[3] if a function f is H-periodic then it is also H'-periodic for a proper subgroup H' of H. So we want to test for bigger subgroups first.

[4] We know that the number of r is $2^{O(n^2)}$ since any H_i is generated by a set of at most n elements of G

Lemma 1. *If f is H_i-periodic, then*

$$\mathsf{Test_i}\,|\Psi_{init}\rangle = |i\rangle\,|1\rangle \otimes \left(\frac{1}{\sqrt{N}}\sum_{g\in G}|g\rangle\,|f(g)\rangle\right)^{\otimes s}$$

Proof. First, we realize that if f is H_i-periodic then s subgroup registers are in superposition of coset states $|tH_i\rangle = \frac{1}{\sqrt{|H_i|}}\sum_{h\in H_i}|th\rangle$ for $t \in T_i$, a translation of H_i. Also, f being H_i-periodic implies that $f(t) = f(th)$ for all $t \in T_i$ and $h \in H_i$. So the state $\frac{1}{\sqrt{N}}\sum_{g\in G}|g\rangle\,|f(g)\rangle = \frac{1}{\sqrt{N}}\sum_{t\in T_i}|tH_i\rangle\,|f(g)\rangle$ lives in $+1$-eigenspace of $P_{1,i}$, and hence $P_{s,i}$ leaves the s couplets untouched. Thus, the lemma follows. $\square$

At the end of the day, what we want to do is to apply the unitary Test to the initial state $|\Psi_{init}\rangle$ to get $|\Psi_{final}\rangle$. Then, we measure the first register of $|\Psi_{final}\rangle$ to get the subgroup index v, and if $1 \le v \le r$ we output a generating set for H_i, otherwise we output 1_G. But our output may be a wrong answer.
As we iterate through r tests for the subgroups, we would wish to only alter the state marginally so that it is safe to continue to test for the next H_{i+1} subgroup.

Lemma 2. *If f is not H_i-periodic, then the distance $\left|(\mathsf{Test_i}\,|\Psi_{init}\rangle) - |\Psi_{init}\rangle\,\right|$ is at most $\frac{2}{2^{s/2}}$.*

The next lemma follows since distances add up linearly.

Lemma 3. *If f is not H_i-periodic for any $1 \le i \le j$, then the distance $\left|\,|\Psi_j\rangle - |\Psi_{init}\rangle\,\right|$ is at most $\frac{2j}{2^{s+2}}$.*

At the beggining in the Theorem, we stated that the error probability is exponential. Great news is that we can make the algorithm exact by the use of classical precomputing and amplitude amlification.
First, we partition the set of subgroups $\{H_1, H_2, \ldots, H_r\}$ into $Y_{1/4}$ and $Y_{3/4}$. We'll look at a new algorithm called $\mathsf{ExactTest}$ that identifies which of the partition the hidden subgroup belongs to.

Lemma 4. *Consider measuring the ancilla qubit of the state $\mathsf{ExactTest}(|\Psi_{init}\rangle \otimes |0\rangle)$. The probability that the outcome of this measurement is 1 is 3/4 if the hidden subgroup H is in $Y_{3/4}$, and it is 1/4 if H is in $Y_{1/4}$.*

In order to describe what $\mathsf{ExactTest}$ is, we need to define few things. Let $Prob[H_i|H]$ be the probability that the measurement outcome of the first register of $|\Psi_{final}\rangle$ is i, conditioned on the hidden subgroup being H. Let M be an $r \times r$ matrix over $[0,1]$ with each row and column indexed by a subgroup. Let entry (H, H_i) of M be $Prob[H_i|H]$. Let y be an $r \times 1$ vector with entries from $\{1/4, 3/4\}$ and each entry indexed by a subgroup. Let $x = M^{-1}y$. Every entry of x is in $[0,1]$ for $r \ge 4$.
Now we define $\mathsf{ExactTest}$

$$\mathsf{ExactTest} = \mathsf{R} \cdot (\mathsf{Test} \otimes \mathsf{I})$$

When we apply ExactTest to the state $|\Psi_{init}\rangle \otimes |0\rangle$, Test is applied to the state $|\Psi_{init}\rangle$ and leaves the ancilla unchanged. Then, R is applied, which is unitary that transforms the ancilla qubit $|0\rangle$ into $\sqrt{1-x_i}\,|0\rangle + \sqrt{x_i}\,|1\rangle$, conditioned on the output register holding the subgroup index i. Thus, the probability that the measurement outcome of the ancilla qubit being 1 is $\sum_i x_i Prob[H_i|H_v]$, which is precisely the entry y_v of y, where H_v is the hidden subgroup. So we just need to set $y_v = 3/4$ if $H_v \in Y_{3/4}$ or set $y_v = 1/4$ if $H_v \in Y_{1/4}$. This proves the lemma

The lemma showed us that we can distinguish between the two sets $Y_{3/4}$ and $Y_{1/4}$ with probabilites 3/4 and 1/4, respectively. Now by using amplitude amplification, we can alter these probabilities into being 0 and 1. Hence, we can distiguish between the two sets. Applying binary search on the set of subgroups, varying the choices of $Y_{3/4}$ and $Y_{1/4}$, we can find the hidden subgroup with certainty.

3 Shor's algorithm reduct to HSP problem of $\mathbb{Z}_{\mathbb{N}}$

Shor's algorithm reduce the problem of factorization of a composite natural number $\mathbb{N}$ to finding the order of an arbitrary non-identity element in $\mathbb{Z}_{\mathbb{N}}$.

Definition 4. A group $\mathbb{Z}_{\mathbb{N}}$ is the set of remainders of a natural number N, up to congruence class.

Definition 5. Order of an element a, where $gcd(a, N) = 1$, in $\mathbb{Z}_{\mathbb{N}}$ is defined by the smallest natural number r, that $a^r \equiv 1 mod_N$.

Then by Lagrange's theorem, the order of all units in $\mathbb{Z}_{\mathbb{N}}$ divide $\phi(N)$, the Euler function value of N, that is less than N, when N is greater than one. The Shor's algorithm begin with choose an arbitrary number in $a \in \{2, ...,$N-1$\}$, then compute the $gcd(a, N)$, if it is not 1, then we already have a non-trivial divisor of N, if it is not one, then we apply it to oder finding algorithm to find the order.Then we get:

$$\begin{aligned} a^r &\equiv 1 mod_N \\ &\Rightarrow (a^{\frac{r}{2}-1})(a^{\frac{r}{2}}+1) \end{aligned}$$

Then if $N|a^{\frac{r}{2}-1}$, implies that $a^{\frac{r}{2}-1} mod_N \equiv 1 mod_N$, then r is not the period, this cannot happen. Then N must divide $a^{\frac{r}{2}+1}$, then compute $gcd(a^{\frac{r}{2}-1}, N)$ to get a non-trivial divisor of N.

In this process the quantum order finding algorithm finds the period of this function:

$$f : \mathbb{N} \to \mathbb{N}$$

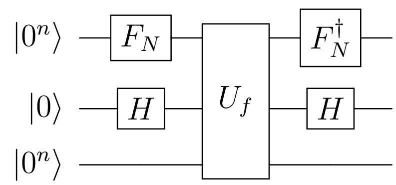
Then we have a function $f(a) = x^a \ mod_N$ and $f(a) = f(b)$ iff $a = b + rk$, where k is an arbitrary integer. Thus it hides the subgroup of of $\mathbb{Z}_{\mathbb{N}}$ which is generated by r. If the function $f : \mathbb{N} \to \mathbb{N}$ has period r, then $f(a) = f(b)$ iff a and b are in the same coset generated by r, i.e. $a \in b + < r >$.

4 Dihedral Group HSP

In order to solve Dihedral Group HSP, we first need to characterize the subgroups of the Dihedral Group $D_N = \{r, s | ord(r) = N, ord(s) = 2, srs = r^{-1}\}$. First, there are the cyclic subgroups generated by the set $\{r^k | k \in \mathbb{Z}_N\}$, which are normal in D_N. There are also dihedral subgroups, which are of the form D_m, where m divides N. And the other subgroups are generated by sr^k and are of order 2.
In 1998, Ettinger and Hoyer showed that it is possible to reduce the problem of solving the hidden subgroup problem on D_N with hiding function f to calculating k assuming the hidden subgroup is generated sr^k. The reason is fairly simple. If the hidden subgroup is a cyclic subgroup of D_N, then it is normal in D_N and can be calculated in polynomial time using previous results. If it is a dihedral subgroup D_m, then the hidden subgroup itself has a cyclic subgroup - it hides a cyclic subgroup $\langle r^k \rangle$. We take the factor group $D_N / \langle r^k \rangle$ after calculating k, and we find the hidden subgroup that remains $D_m / \langle r^k \rangle$, which is just an order 2 subgroup. To recap, first we try to find if there is a cyclic subgroup that is hidden. If $\langle r^a \rangle$ is hidden, we calculate a using previously known results about finding hidden normal subgroups. After that, we take the factor group $D_N / \langle r^a \rangle$ and see if the function f hides an order 2 subgroup generated by sr^k or if only the trivial subgroup remains. If both a cyclic and an order 2 subgroup was detected, we have a hidden dihedral subgroup. Otherwise, it is either a cyclic or an order 2 subgroup that is hidden and we have detected it. Now we move to the algorithm for detecting an order 2 subgroup.

In order to solve Dihedral Group HSP, we first need to characterize the subgroups of the Dihedral Group $D_N = \{r, s | ord(r) = N, ord(s) = 2, srs = r^{-1}\}$. First, there are the cyclic subgroups generated by the set $\{r^k | k \in \mathbb{Z}_N\}$, which are normal in D_N. There are also dihedral subgroups, which are of the form D_m, where m divides N. And the other subgroups are generated by sr^k and are of order 2.
In 1998, Ettinger and Hoyer showed that it is possible to reduce the problem of solving the hidden subgroup problem on D_N with hiding function f, to calculating k assuming the hidden subgroup is generated by sr^k. The reason is fairly straightforward. If the hidden subgroup is a cyclic subgroup of D_N, then it is normal in D_N and can be calculated in polynomial time using previous results. If it is a dihedral subgroup D_m, then the hidden subgroup itself has a cyclic subgroup - f hides a cyclic subgroup $\langle r^k \rangle$. We take the quotient group $D_N / \langle r^k \rangle$ after calculating k, and we find the hidden subgroup that remains $D_m / \langle r^k \rangle$, which is just an order 2 subgroup. To recap, first we try to find if there is a cyclic subgroup that is hidden. If $\langle r^a \rangle$ is hidden, we calculate a using previously known results about finding hidden normal subgroups. After that, we take the quotient group $D_N / \langle r^a \rangle$ and see if the function f hides an order 2 subgroup of this new quotient group, generated by sr^k, or if only the trivial subgroup remains. If both a cyclic and an order 2 subgroup was detected, we have a hidden dihedral subgroup. Otherwise, it is either a cyclic or an order 2 subgroup that is hidden and we have detected it. Now we move to the algorithm for detecting an order 2 subgroup.

The standard procedure for solving HSP, used in Shor's algorithm for $\mathbb{Z}_N^\times$, Simon's algorithm mod p (from our homework) over $\mathbb{Z}_p \times \mathbb{Z}_p$, and others, is to obtain a superposition over all possible states, then apply function unitary and apply the inverse of the unitary that gave us the superposition of all states. This is the same for HSP on the dihedral group. An element of $s^b r^a \in D_N$ will be represented as $|a\rangle\,|b\rangle$, where $b \in \{0,1\}$ and $a \in \mathbb{Z}_N$. Then a will take $n = \lceil \log(N) \rceil$ qubits to represent, and b will take 1. We also want to be able to store output, so we represent output in another n qubits, so we start with $|0^n\rangle\,|0\rangle\,|0^n\rangle$. The circuit we apply is



where our unitary U_f takes $|a\rangle\,|b\rangle\,|c\rangle \to |a\rangle\,|b\rangle\,|c + f(a,b)\rangle$. We also have F_N is the quantum Fourier transform for $\mathbb{Z}_N$. After applying the quantum circuit, we measure the first two registers (everything but the function output). These states collapse in a similar way to Simon's algorithm's collapsing, and we are in business! In the end, measuring registers 1 and 2 gives

$$\Pr[|a\rangle\,|0\rangle] = \frac{1}{N}(\cos^2(\frac{\pi k a}{N}))$$
$$\Pr[|a\rangle\,|1\rangle] = \frac{1}{N}(\sin^2(\frac{\pi k a}{N}))$$

We make $m = 2\lceil 64 \ln(N) \rceil$ samples using this method, and collect all of those samples with the most numerous final bit (i.e. at least $m/2$ will have final bit 1 or 0). Call this number m', and the samples $z_1, \cdots, z_{m'}$. Thanks to the distribution, and a probabilistic result from Hoeffding, we have a method of determining k. The method is that, with high probability, $k' = k$ or $k' = N - k$ will satisfy

$$\sum_{i=1}^{m'} \cos(2\pi k' z_i) > \frac{m}{4}$$

and any other values of k' will satisfy

$$\sum_{i=1}^{m'} \cos(2\pi k' z_i) < \frac{m}{4}$$

Then by enumerating through $k' = 1, \cdots, N/2$, we can find a value of k' that satisfies either $k' = k, N - k$, so we need to check just 3 values of f after all the sampling in order to determine if we've found the correct k.

It is known that there is a reduction from solving HSP for the Dihedral group using sampling as in this algorithm, to solve the shortest vector problem on lattices. SVP is significant as it commonly studied as a post-quantum cryptographic problem.

References

[1] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. *A quantum algorithm for computing the unit group of an arbitrary degree number field*. 2014 ACM Symposium on Theory of Computing, 2014.

[2] Oded Regev. *A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space*. arXiv:quant-ph/0406151, 2004.

[3] Oded Regev. *Quantum Computation and Lattice Problems*. arXiv:cs/0304005, 2003.

[4] Mark Ettinger, Peter Hoyer, and Emanuel Knill. *The quantum query complexity of the hidden subgroup problem is polynomial*. arXiv:quant-ph/0401083, 2004.

[5] Mark Ettinger, Peter Hoyer. *On Quantum Algorithms for Noncommutative Hidden Subgroups*. arXiv:quant-ph/9807029, 1998.

[6] Frédéric Wang. *The Hidden Subgroup Problem*. arXiv:1008.0010, 2010.