# CIS 410 Midterm Report on Hidden Subgroup Problem

Zhimeng Wang, Dongmin Roh, Matthew Jagielski

May 12, 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 $g_1 H = g_2 H$, 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 centainty a hidden subgroup problem of an arbitrary finite group in a polynomail (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 solve the HSP on finite abelian groups in polynomial time, it is possible for quantum computers to factor integers much faster than classical computers can.

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 Midterm Report

## 2.1 Quantum Query Complexity of HSP is polynomial

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 $1 \leq i \leq r$. Also let $N = |G|$ and consider $n = log|G|$ to be the input size.[1]

**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 disctinct cosets of $H$.
A left *translation* of a subgroup $H$ is a subset $T \subseteq G$ such that for any $g \in G$, $g = tk$ for some $t \in T$ and $k \in K$.
We define an operator $\mathsf{Test}$ 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

$$Q_i : \quad \begin{cases} |0\rangle\,|0\rangle & \mapsto \quad |i\rangle\,|1\rangle \\ |v\rangle\,|l\rangle & \mapsto \quad |v\rangle\,|l+1\rangle\,, \qquad \text{if } l > 0 \end{cases}$$

[1]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 $G$

# 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.