CIS 410 Project Proposal on Hidden Subgroup Problem

zhmeng wang, Dongmin Roh,Matthew Jagielski

April 29, 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 problem 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.

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 very important for postquantum cryptography.

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 References

- A quantum algorithm for computing the unit group of an arbitrary degree number field, by Kirsten Eisentrger, Sean Hallgren,Alexei Kitaev and Fang Song.
- A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space by Oded Regev
- QUANTUM COMPUTATION AND LATTICE PROBLEMS by Oded Regev

3 Timeline

Midterm Report: We will explore and identify the basic idea of the HSP problem and then review the thinking of the polynomial time algorithm to solve HSP problem. We want to understand the problem well and know the quantum algorithms that approach its solution by the midterm report. We will also know how the SVP reduction is done, as well as understanding other impacts for HSP on computer science and math.
Final Presentation: Due by final presentation, I want to present a sketch of the construction of HSP on general abelian groups and to clarify its usage on main ideals of the generating set of general abelian groups and the vector spaces over a finite field. This includes being able to give intuition for the parts of the algorithms and for understanding the problems, as well.