The Hidden Subgroup Problem in Special Classes of Nil-3 Groups

Paul Gustafson
Department of Mathematics
Texas A&M University
pgustafs@math.tamu.edu

Julia Plavnik
Department of Mathematics
Texas A&M University
julia@math.tamu.edu

Qing Zhang
Department of Mathematics
Texas A&M University
zhangqing@math.tamu.edu

***Abstract*—We summarize the important techniques in Ivanyos, Sanselme, and Santha's solution [4] to the hidden subgroup problem (HSP) for nilpotent groups of class 2. We plan to extend these techniques to some simple examples of nilpotent groups of class 3 – for example, a semidirect product of a cyclic group and the Heisenberg group of a finite field.**

I. Description of the problem

Problem: Solve the HSP for $H \leq G$, where G is a nil-2 group.

II. Discussion of background

A. Preliminaries

Here is a summary about the preliminaries for HSP and nilpotent groups:

1) There is an extension of the standard algorithm for HSP in terms of quantum hiding function, which is given in section 2.1.
2) A group G is called nilpotent if its lower central series stops in $\{e\}$ after finitely many steps.
3) A nilpotent group G is said to be a *nil-n* group if it is of class at most n.
4) A group G is a nil-2 group if G' is contained in the center of G, where G' is the derived subgroup of G.
5) If G is a p-group of exponent p and of class 2, the structure of G, G' and G/G' is well studied and is summarized in section 2.3 in this paper.
6) If G is a p-group of exponent p and of class 2, then there exist a class of automorphisms ϕ_j with certain nice properties. These automorphisms are used in the quantum algorithm described in this paper.

B. Related Work

The HSP can be solved efficiently for abelian groups using quantum algorithms. Many efforts have been made to solve the HSP in finite non-abelian groups. Many groups where the HSP have been efficiently solved are somehow groups that are very close to be abelian groups, e.g. [1], [3] and [2].

Some previous work for this paper have been done is about solving the HSP for extraspecial groups [4], which are examples of nil-2 groups. This paper follows a similar procedure, which uses theoretical tools to reduce the problem to the HSP in abelian groups.

III. Summary of Nil-2 HSP Algorithm

A. Reduction Steps

1) Calculate the refined polycyclic representation of G.
2) Reduce to HSP in nil-2 p-groups
3) Reduce to case where H is either trivial or order p
4) Reduce to case where G has exponent p.
5) Reduce to finding a quantum hiding function for HG'
6) Reduce to finding an appropriate triple
7) Reduce to solving a large system of linear and quadratic equations

B. Quantum Algorithm

All of the above steps have efficient classical algorithms, except for the step of generating a quantum hiding function for HG' given an appropriate triple, so we will focus on this step. The following is a summary of this algorithm:

1) Compute the superposition $\sum_{u \in G'} |u\rangle \, |aHG'_u\rangle$ for random $a \in G$, where $G_u = DFT(|u\rangle)$.
2) Do the last step n times in parallel for some large n
3) Solve the system of equations to get $\bar{j} \in (\mathbf{Z}_p)^n$
4) $\left|\Psi_g^{\bar{a},\bar{u},\bar{j}}\right\rangle = \bigotimes_{i=1}^n \left|a_i HG'_{u_i} \phi_{j_i}(g)\right\rangle$ as a function of $g \in G$ is a hiding function for HG', where ϕ_j are nice automorphisms of G.

The following properties of the automorphisms ϕ_j are used in the proof:

1) $|aHG'_u\rangle$ is an eigenvector for right multiplication by $\phi_j(g)$
2) ϕ_j maps HG' to HG'

References

[1] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. *Quantum mechanical algorithms for the non- abelian Hidden Subgroup Problem*. In Proc. 33rd ACM STOC, pages 6874, 2001.

[2] C. Moore, D. Rockmore, A. Russell, and L. Schulman. *The power of basis selection in Fourier sampling: Hidden subgroup problems in affine groups*. In Proc. 15th ACM-SIAM SODA, pages 11061115, 2004.

[3] M. Rötteler and T. Beth. *Polynomial-time solution to the Hidden Subgroup Problem for a class of non-abelian groups*. `http://xxx.lanl.gov/abs/quant-ph/9812070`

[4] G. Ivanyos, L. Sanselme, and M. Santha. *An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups*. Proc. 24th STACS, LNCS vol. 4393, pages 586597, 2007.