Quantum Solution to the Hidden Subgroup Problem for Poly-Near-Hamiltonian Groups

Dmitry Gavinsky[1] *

[1] *Department of Computer Science, University of Calgary. Calgary, Alberta, Canada, T2N 1N4*

Abstract. The *Hidden Subgroup Problem (HSP)* has been widely studied in the context of quantum computing and is known to be efficiently solvable for Abelian groups, yet appears to be difficult for many non-Abelian groups. An *efficient algorithm for* HSP is one that runs in time polynomial in n, where $n = \log|G|$.

For any subgroup H of G, let $N(H)$ denote the normalizer of H. Let M_G denote the intersection of all normalizers in G (i.e., $M_G = \cap_{H \le G} N(H)$). M_G is always a subgroup of G and the size of $[G : M_G]$ can be taken as a kind of measure of how non-Abelian G is ($[G : M_G] = 1$ for Abelian groups). This was considered by Grigni, Schulman, Vazirani and Vazirani, who showed that, whenever $[G : M_G] \in \exp(O(\log^{1/2} n))$, the corresponding HSP can be solved efficiently, assuming that the Quantum Fourier Transform (QFT) over G can be performed efficiently. We extend this result by showing that, whenever $[G : M_G] \in \mathrm{poly}(n)$, the corresponding HSP can be solved efficiently, assuming that the QFT over G can be performed efficiently (and also a slightly more general version of this result). We also show that the assumption that the QFT is efficient over G may be replaced by another, apparently less strict, assumption.

Keywords: Hidden Subgroup Problem, Quantum Algorithms

1 Introduction

The *Hidden Subgroup Problem (HSP)* has been studied by several authors in the context of Quantum Computing (e.g., see [1], [2], [3], [5] and [4]).

The problem is defined as follows. We are given a (quantum) oracle for some function f, defined over elements of G and satisfying the following conditions: Over all members of a *hidden subgroup* $H \le G$, f is constant; as well, the function is constant for the elements of each left coset of H. At the same time, the function is distinct for distinct cosets.

To solve the HSP in this case means to construct a generating set for H, being provided with access to an oracle computing f. For a problem to be reducible to the HSP means that the oracle may be replaced by an efficient algorithm computing such a function f, and a generating set for H would provide a solution to the original problem. In particular, the HSP is known to be quantum solvable for the case of Abelian groups. The known quantum algorithm solving the HSP for Abelian G is based on the Quantum Fourier Transform (QFT) over G.

As a possible extension, Grigni, Schulman, Vazirani and Vazirani [4] show solution to the case of *almost Abelian* groups, defined as follows:

Let G be a group under consideration, then for any $H \le G$ we use the following notation for the *normalizer* of H:

$$N(H) \stackrel{def}{=} \left\{ g \in G \,\middle|\, gHg^{-1} = H \right\}.$$

We define M_G to be the intersection of all the normalizers:

$$M_G \stackrel{def}{=} \bigcap_{H \le G} N(H).$$

Define a parameter k_G:

$$k_G \stackrel{def}{=} [G : M_G].$$

Then, according to [4], a group G is *almost Abelian* if $k_G \in \exp(O(\log^{1/2} n))$, for $n = \log|G|$.

We extend the notation and define a group G to be k_G*-near-Hamiltonian*. In particular, G is *(poly-) near-Hamiltonian* if $k_G \in poly(n)$.

1.1 Our results

We give an efficient quantum solution to the HSP for the case of near-Hamiltonian groups. Our final algorithm solves a slightly more general case, when the hidden subgroup H satisfies: $[G : HM_G] \in poly(n)$.

We also give a solution which does not assume that the QFT over G can be performed efficiently. Instead, it is based on a subroutine solving the HSP for *Hamiltonian groups*, which are defined as the groups possessing only normal subgroups. An efficient quantum solution to the HSP for Hamiltonian groups has been given by Hallgren, Russell and Ta-Shma in [5].

1.2 Notation and Assumptions

For the constructions of this paper, all the subgroups are represented by (arbitrary) generating sets. We assume that under such representation subgroup membership can be efficiently tested for any group element.

We will use the notation $A \le B$ for groups A and B to say that A is a subgroup of B. By $A \trianglelefteq B$ we will mean that A is normal in B. By $A < B$ we will mean that $A \le B$ and $A \ne B$. If A is a subset of B, we denote this situation by $A \subseteq B$; in this case by $\langle A \rangle_B$ we mean the closure of A in B (the subscript $_B$ will be omitted when is clear from the context). For a group G and some element $x \in G$, we denote by $o(x)$ the order of x in G.

Let G be any group. We denote by $NHS(A)$ for some $A \le G$ the "standard" (e.g., see [4]) algorithm solving the normal HSP for A. For successful execution of $NHS(A)$ one has to be able to efficiently compute QFT over A.

*gavinsky@cpsc.ucalgary.ca

For simplicity we assume that $NHS(A)$ is always correct and if a proper solution has not been found by $NHS(A)$ it returns a "failure" message. In fact, the known algorithm is probabilistic and has exponentially low probability to fail; however, since our algorithms are efficient and use $NHS(A)$ at most polynomial number of times, our assumption of $NHS(A)$ correctness is false with only exponentially small probability for a single execution of each one of our algorithms.

For a quotient group $A = G/N$ we will not distinguish between element of A and cosets of N in G (i.e., we view the elements of A as subsets of G). For convenience we will use the following shorthand notation:

$$\mathbf{U}_A(x) \stackrel{def}{=} \bigcup_{t \in \langle x \rangle_A} t,$$

for any $x \subseteq A$, as well as any $x \in A$ (in the latter case $\langle x \rangle_A$ actually means $\langle \{x\} \rangle_A$).

2 HSP for Near-Hamiltonian Groups

In this section we solve the HSP for near-Hamiltonian groups, i.e., we assume that $[G : M_G] \in poly(n)$.

The following algorithm solves the problem (Figure 1).

$HS_1(G)$
set: $T = \emptyset$
for each $x \in G/M_G$ **do**
  set: $U = \mathbf{U}_{G/M_G}(x)$
  if $NHS(U)$ *is successful* **then**
    if $\langle NHS(U) \rangle \cap x \neq \emptyset$ **then**
      set: $T = T \cup \{x\}$
end-for
return $NHS(\cup_{t \in T} t)$

Figure 1: Algorithm $HS_1(G)$ for solving the HSP for a near-Hamiltonian group G.

In order to construct $HS_1(G)$ we have made some assumptions (similar to those made in [4]):

1. We assume that for any $U = \mathbf{U}_{G/M_G}(x)$ (where $x \in G/M_G$), we can efficiently execute $NHS(U)$; in particular, this requires to be able to efficiently compute the corresponding Quantum Fourier Transform $QFT(U)$.

2. We assume that we can efficiently iterate through all $x \in G/M_G$.

In the paper we show that these both assumptions are not essential and may be either removed or "relaxed".

3 Finding the Hidden Subgroup H, When $[G : HM_G] \in poly(n)$

In this section we show that our approach can be used to find efficiently the hidden subgroup H, when $[G : HM_G] \in poly(n)$. We denote by d a corresponding (polynomial in n) upper bound on $[G : HM_G]$.

$HS_2(G, d, \delta)$
1. **set:** $T = \emptyset$
2. **set:** $n = \log |G|$
3. **repeat** $4nd \ln(1/\delta)$ **times**
4.   **draw uniformly:** $x \in G/M_G$
5.   **set:** $U = \mathbf{U}_{G/M_G}(x)$
6.   **if** $NHS(U)$ *is successful* **then**
7.   **if** $\langle NHS(U) \rangle \cap x \neq \emptyset$ **then**
8.   **set:** $T = T \cup \{x\}$
9. **end-repeat**
10. **return** $NHS(\mathbf{U}_{G/M_G}(T))$

Figure 2: Algorithm $HS_2(G, d, \delta)$ for solving the HSP with confidence $1 - \delta$ for the group G, when the hidden subgroup H satisfies: $[G : HM_G] \leq d$.

The algorithm (denoted by $HS_2(G, d, \delta)$) follows in Figure 2.

In the paper we show that the condition in line 7 of HS_2 may be efficiently checked and the whole algorithm is efficient.

In Section 2 we list two assumptions we are making for the construction of HS_1. For HS_2 assumption 2 is no longer needed (HS_2 does not iterate through all $x \in G/M_G$). What is more, in order to pick (uniformly) a random element from G/M_G, it is enough to sample a random element from $x \in G$ and to consider the M_G's coset which contains this x.

4 Acknowledgments

I express my appreciation to Richard Cleve for valuable comments and suggestions.

References

[1] R. Beals. Quantum computation of Fourier transforms over symmetric groups. *Proceedings of the 29th Symposium on Theory of Computing, pp. 48-53*, 1997.

[2] M. Ettinger and P. Hoyer. On quantum algorithms for noncommutative hidden subgroups. *Proceedings of the 16th Symposium on Theoretical Aspects of Computer, pp. 478-487*, 1999.

[3] M. Ettinger, P. Hoyer and E. Knill. Hidden subgroup states are almost orthogonal. *http://arxiv.org, quant-ph/9901034*, 1999.

[4] M. Grigni, L. J. Schulman, M. Vazirani and U. V. Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. *Proceedings of the 33th Symposium on Theory of Computing, pp. 68-74*, 2001.

[5] S. Hallgren, A. Russell and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. *Proceedings of the 32nd Symposium on Theory of Computing, pp. 627-635*, 2000.