

# Quantum Hidden Subgroup Algorithms: The Devil Is in the Details

Samuel J. Lomonaco, Jr.<sup>a</sup> and Louis H. Kauffman<sup>b</sup>

<sup>a</sup>Department of Computer Science and Electrical Engineering, University of Maryland

Baltimore County, 1000 Hilltop Circle, Baltimore, Maryland 21250,USA

<sup>b</sup>Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 South Morgan Street, Chicago, Illinois 60607-7045,USA

## ABSTRACT

We conjecture that one of the main obstacles to creating new non-abelian quantum hidden subgroup algorithms is the correct choice of a transversal.

## 1. INTRODUCTION

New quantum algorithms are crucially needed to demonstrate that future quantum computers will be more than highly specialized machines, but instead highly versatile general purpose devices. Unfortunately, the current choice of quantum algorithms available for future quantum computing devices is surprisingly meager. With some minor (but important) exceptions, there are only three available classes of quantum algorithms, namely:

- 1) Quantum hidden subgroup (QHS) algorithms, i.e., Shor/Simon-like algorithms,
- 2) Amplitude amplification algorithms, i.e., Grover-like algorithms, and
- 3) Quantum algorithms that simulate quantum systems on a quantum computer.

In this paper, we focus on the development of new non-abelian QHS algorithms because of their tantalizing promise of exponential speedup over existing classical algorithms. For example, should there be a major breakthrough in non-abelian QHS algorithm development, then there is the enticing possibility that it might be possible to develop a polynomial-time QHS algorithm for the graph isomorphism problem.

In spite of the efforts of many researchers, the number of new non-abelian QHS algorithms is very small and scattered. Why is it so difficult to generalize QHS algorithms to non-abelian groups?

Before we can even guess at an answer to this question, we first need to define what we mean by a quantum hidden subgroup algorithm.

---

Further author information: S.J.L., Jr. E-mail: Lomonaco@umbc.edu; L.H.K. E-mail: kauffman@uic.edu

## 2. THE QUANTUM HIDDEN SUBGROUP ALGORITHM PARADIGM

We begin by first defining the classical hidden subgroup problem:

**HIDDEN SUBGROUP PROBLEM.** Given a group  $G$  and a map  $f : G \rightarrow H$  (not necessarily a morphism) of  $G$  into a group  $H$ , is it possible to find an invariant subgroup  $K$  of  $G$  such that the map  $f$  can be factored into the composition  $f = \iota \circ \gamma$  of two maps  $\gamma : G \rightarrow G/K$  and  $\iota : G/K \rightarrow H$ , where  $\gamma$  denotes the natural epimorphism, and where  $\iota$  denotes an injection. The subgroup  $K$  is called a *hidden subgroup*.

The quantum analog of the classical hidden problem is defined as follows:

**GENERIC QUANTUM HIDDEN SUBGROUP PROBLEM.** Let  $\mathcal{H}_G$  and  $\mathcal{H}_H$  be Hilbert spaces with respective orthonormal bases

$$\{|g\rangle : g \in G\} \text{ and } \{|h\rangle : h \in H\} .$$

Assume that  $f : G \rightarrow H$  is given as a unitary transformation

$$\begin{aligned} U_f : \mathcal{H}_G \otimes \mathcal{H}_H &\longrightarrow \mathcal{H}_G \otimes \mathcal{H}_H \\ |g\rangle |h\rangle &\longmapsto |g\rangle |f(g)h^{-1}\rangle \end{aligned}$$

Determine the hidden subgroup of  $f$  by making as few queries as possible to the blackbox  $U_f$ .

We can now in turn define what we mean by a QHS algorithm that solves the above QHS problem:

The **GENERIC QUANTUM HIDDEN SUBGROUP (QHS) ALGORITHM** is essentially (ignoring many subtleties) the following:

- **STEP 0.** Initialize two registers  $|\text{LEFT-REG}\rangle$  in  $\mathcal{H}_G$  and  $|\text{RIGHT-REG}\rangle$  in  $\mathcal{H}_H$  to produce the initial state  $|\psi_0\rangle = |0\rangle |1\rangle$ , assuming additive notation for  $G$ , and multiplicative notation for  $H$ .
- **STEP 1.** Apply the Fourier transform  $\mathcal{F}_G$  to the left register.
- **STEP 2.** Apply the unitary transformation  $U_f$ . (As mentioned by Shor,<sup>17</sup> there is no need to measure the right register.)
- **STEP 3.** Again apply the Fourier transform  $\mathcal{F}_G$  to the left register.
- **STEP 4.** Measure the left register.
- **STEP 5.** Repeat Steps 0 through 4 until enough measurements have been made to determine the hidden subgroup.

Both Jozsa<sup>5</sup> and Kitaev<sup>6</sup> have noted that Simon's quantum algorithm and Shor's quantum factoring algorithms can be viewed as instances of the same generic quantum hidden subgroup algorithm for abelian groups. Simon's algorithm determines a hidden subgroup of the direct sum of cyclic groups of order 2. Shor's algorithm determines a hidden subgroup of the infinite cyclic group.

But can the generic abelian hidden subgroup algorithm be extended to a larger class of groups? If it could be extended to a large enough class of non-abelian groups, then there is a strong possibility that a polynomial-time

quantum algorithm for the graph isomorphism problem could be found in this way. (For an in depth study of the graph isomorphism problem, see, for example, Hoffman.<sup>4</sup> For applications, see, for example, Tarjan.<sup>19</sup> For a discussion as to how to extend the quantum hidden subgroup problem to non-abelian groups, see for example Lomonaco.<sup>13</sup> )

But once again, we ask:

Why has it been so difficult to create new non-abelian QHS algorithms?

We can not give a complete answer to this question. But we can give some clues as to why non-abelian QHS algorithm development has been so difficult.

### 3. “THE DEVIL IS IN THE DETAILS.”

“The devil is in the details.” By that we mean the following:

A number of subtleties were ignored in the above description of the generic QHS algorithm. These subtleties become absolutely crucial when one tries to extend the generic QHS algorithm to a larger class of non-abelian groups.

There is simply not enough space to discuss all the important subtleties in regard to the generic QHS algorithm. So we will focus on only one, which the authors believe has been ignored by many in the research community.

Contrary to conventional wisdom, Simon’s and Shor’s algorithms are far from the same generic QHS algorithm. To say so is a gross oversimplification. There are crucial differences. Shor’s algorithm, unlike Simon’s, outputs group characters which are approximations to the group characters actually sought.

More specifically, to find a hidden subgroup of  $f : G \rightarrow H$ , Shor’s algorithm selects a “large” epimorphic image  $\nu : G \rightarrow Q$  for “approximating”  $f$ . Crucially, Shor’s algorithm also selects a “correct” transversal map  $\tau : Q \rightarrow G$ , where a transversal  $\tau : Q \rightarrow G$  is an injection such that  $\nu \circ \tau = id_Q$ , where  $id_Q$  denotes the identity map on  $Q$ .

Once the transversal  $\tau$  has been selected, we can define an approximation  $\tilde{f}$  to  $f$  by  $\tilde{f} = f \circ \tau$ . We can now use the Fourier transform of  $\tilde{f}$  associated with the group  $Q$  to find the hidden subgroup of  $f$ . Thus, Shor’s algorithm outputs random group characters of  $Q$  which are approximations to the group characters of  $H$ .

We emphasize one key point here:

The selection of the transversal  $\tau : Q \rightarrow G$  .

On the one hand, a good choice will produce an efficient algorithm. On the other hand, a bad choice will lead to an inefficient algorithm. Unfortunately, Shor’s original algorithm gives no hint as to how to choose the transversal  $\tau : Q \rightarrow G$  generically. This, of course, is only one of the difficulties encountered in trying to generalize Shor’s algorithm to non-abelian groups. But it appears to be a crucial one that has, for the most part, been ignored. The significance of the correct choice of a transversal is made transparent by Lomonaco and Kauffman,<sup>11</sup> where the correct transversal for the abelian QHS algorithm is found to be what is called in their paper a Shor transversal.

Another obstacle to the development of new non-abelian QHS algorithms is the time complexity of the non-abelian Fourier transform.

## 4. THE NON-ABELIAN FOURIER TRANSFORM

The Fourier transform on non-abelian groups is defined as follows:

Let  $G$  be a finite non-abelian group, and let  $\pi^{(1)}, \pi^{(2)}, \dots, \pi^{(k)}$  be a complete set of distinct irreducible representations of the group  $G$ .

Each irreducible representation is a morphism  $\pi^{(i)} : G \rightarrow \text{Aut}(W_i)$  from  $G$  to the group of automorphisms of the representation space  $W_i$ . Let  $\pi^{(i)\#} : G \rightarrow \text{Aut}(W_i^*)$ , denote the corresponding contragredient representation, where  $W_i^*$  is the dual  $W_i$ . Extend the representation  $\pi^{(i)\#} : G \rightarrow \text{Aut}(W_i^*)$  to the group ring, i.e., to  $\pi^{(i)\#} : \mathbb{C}G \rightarrow \text{End}(W_i^*)$ , where  $\mathbb{C}G$  denotes the group ring of  $G$  over the complex numbers  $\mathbb{C}$ , and where  $\text{End}(W_i^*)$  denotes the ring of endomorphisms of  $W_i^*$ . Then the *non-abelian Fourier transform*  $\mathcal{F}_G$  on the group  $G$  is defined as

$$\mathcal{F}_G = \bigoplus_{i=1}^k \pi^{(i)\#} : \mathbb{C}G \rightarrow \bigoplus_{i=1}^k \text{End}(W_i^*) \quad ,$$

where  $\bigoplus$  denotes the direct sum.

The above Fourier transform can be expressed more explicitly, but less transparently, in terms of matrices.

The algorithmic time complexity of the non-abelian Fourier transform depends to a large extent on the basis chosen to express the Fourier transform in terms of matrices. But this complexity will depend on which transversal  $\tau : Q \rightarrow G$  is chosen for the non-abelian QHS algorithm!

## 5. CONCLUSION

In this paper, we conjecture that one of the main obstacles to creating new non-abelian QHS algorithms for the hidden subgroup problem  $f : G \rightarrow H$  is the correct choice for the transversal  $\tau : Q \rightarrow G$ .

## 6. ACKNOWLEDGEMENTS

This work was supported by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement F30602-01-2-05022. Some of this effort was also sponsored by the National Institute for Standards and Technology (NIST). The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright annotations thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Defense Advanced Research Projects Agency, the Air Force Research Laboratory, or the U.S. Government. (Copyright 2004.) The first author would also like to thank the Mathematical Sciences Research Institute (MSRI) at Berkeley, California for its support of this work.

## REFERENCES

1. Ettinger, Mark and Peter Hoyer, *On Quantum Algorithms for Noncommutative Hidden Subgroups*, <http://xxx.lanl.gov/abs/quant-ph/9807029>
2. [Ettinger2] Ettinger, Mark, Peter Hoyer, and Emanuel Knill, *Hidden Subgroup States are Almost Orthogonal*, <http://xxx.lanl.gov/abs/quant-ph/9901034>
3. Ettinger, J. Mark, and Peter Hoyer, *Quantum State Detection Via Elimination*, <http://xxx.lanl.gov/abs/quant-ph/9905099>
4. Hoffmann, Christoph, “*Group-Theoretic Algorithms and Graph Isomorphisms*,” Springer-Verlag (1982).
5. Jozsa, Richard, *Quantum Factoring, Discrete Logarithms and the Hidden Subgroup Problem*, <http://xxx.lanl.gov/abs/quant-ph/0012084>
6. Kitaev, A., *Quantum Measurement and the Abelian Stabiliser Problem*, (1995), <http://arXiv.org/abs/9511026>.
7. Lomonaco, Samuel J., Jr. (editor), “*Quantum Computation*,” AMS PSAPM/58, American Mathematical Society, Providence, RI, (2002).
8. Lomonaco, Samuel J., Jr., and Howard E. Brandt, “*Quantum Computation and Information*,” AMS CONM/305, American Mathematical Society, Providence, RI, (2002).
9. Lomonaco, Samuel J., Jr., and Louis H. Kauffman, *A Continuous Variable Shor Algorithm*, AMS CONM, (to appear 2004). <http://xxx.lanl.gov/abs/quant-ph/0210141>
10. Lomonaco, Samuel J., Jr., *Shor’s Quantum Factoring Algorithm*, AMS PSAPM/58, (2002), 161-180. <http://arXiv.org/abs/quant-ph/0010034>
11. Lomonaco, Samuel J., Jr., and Louis H. Kauffman, *Quantum Hidden Subgroup Algorithms: A Mathematical Perspective*, AMS, CONM/305, (2002), 139-202.
12. Lomonaco, Samuel J., Jr., and Louis H. Kauffman, *Continuous Quantum Hidden Subgroup Algorithms*, SPIE Proc., vol. 5105, (2003), 80-88. <http://xxx.lanl.gov/abs/quant-ph/0304084>
13. Lomonaco, Samuel J., Jr., *The Non-Abelian Fourier Transform and Quantum Computation*, <http://www.msri.org/publications/ln/msri/2000/qcomputing/lomonaco/1/>, (2000), Mathematical Sciences Research Institute (MSRI) Video.
14. Mosca, Michele, and Artur Ekert, *The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer*, <http://xxx.lanl.gov/abs/quant-ph/9903071>
15. Nielsen, Michael A., and Isaac L. Chuang, “*Quantum Computation and Quantum Information*,” Cambridge University Press, (2000).
16. Roetteler, Martin, and Thomas Beth, *Polynomial-Time Solution to the Hidden Subgroup Problem for a Class of Non-Abelian Groups*, <http://xxx.lanl.gov/abs/quant-ph/9812070>
17. Shor, Peter W., *Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. on Computing, 26(5), (1997), 1484-1509. <http://xxx.lanl.gov/abs/quant-ph/9508027>
18. Shor, Peter W., *Introduction to Quantum Algorithms*, AMS PSAPM/58, (2002), 143-160. <http://xxx.lanl.gov/abs/quant-ph/0005003>
19. Tarjan, R.E., *Graph Algorithms in Chemical Computations*, in “*Algorithms in Chemical Computations*,” edited by R.E. Christoffersen, Amer. Chem. Soc. (1977), pp 1-20.
20. Watrous, John, *Quantum algorithms for solvable groups*, <http://arXiv.org/abs/quant-ph/0011023>