IS GROVER'S ALGORITHM A QUANTUM HIDDEN SUBGROUP ALGORITHM ?

SAMUEL J. LOMONACO, JR. AND LOUIS H. KAUFFMAN

ABSTRACT. The arguments given in this paper suggest that Grover's and Shor's algorithms are more closely related than one might at first expect. Specifically, we show that Grover's algorithm can be viewed as a quantum algorithm which solves a non-abelian hidden subgroup problem (HSP). But we then go on to show that the standard non-abelian quantum hidden subgroup (QHS) algorithm can not find a solution to this particular HSP.

This leaves open the question as to whether or not there is some modification of the standard non-abelian QHS algorithm which is equivalent to Grover's algorithm.

CONTENTS

1. INTRODUCTION

Is Grover's algorithm a quantum hidden subgroup (QHS) algorithm ?

We do not completely answer this question. Instead, we show that Grover's algorithm is a QHS algorithm in the sense that it can be rephrased as a quantum algorithm which solves a non-abelian hidden subgroup problem (HSP) on the symmetric group $\mathbb{S}_N$. But we then go on to show that the standard non-abelian QHS algorithm cannot solve the Grover HSP.

This leaves unanswered an intriguing question:

Question. *Is there an extension or modification of the standard non-abelian QHS on the symmetric group S_N which solves the non-abelian HSP associated with Grover's algorithm?*

It should be mentioned that, because of a result of Zalka [31], such an algorithm, if it exists, could not be asymptotically faster than Grover's algorithm.

We hope that the results found in this paper will lead to a better understanding of quantum algorithms.

2. Definition of the hidden subgroup problem (HSP) and hidden subgroup algorithms

What is a hidden subgroup problem ?   What is a hidden subgroup algorithm ?

Definition 1. *A map $\varphi : G \longrightarrow S$ from a group G into a set S is said to have* **hidden subgroup structure** *if there exists a subgroup K_φ of G, called a* **hidden subgroup**, *and an injection $\iota_\varphi : G/K_\varphi \longrightarrow S$, called a* **hidden injection**, *such that the diagram*

$$
\begin{array}{ccc}
G & \xrightarrow{\ \varphi\ } & S \\
{\scriptstyle \nu}\searrow & & \nearrow {\scriptstyle \iota_\varphi} \\
& G/K_\varphi &
\end{array}
$$

is commutative[1], where G/K_φ denotes the collection of right cosets of K_φ in G, and where $\nu : G \longrightarrow G/K_\varphi$ is the natural surjection of G onto G/K_φ. We refer to the group G as the **ambient group** *and to the set S as the* **target set**. *If K_φ is a normal subgroup of G, then $H_\varphi = G/K_\varphi$ is a group, called the* **hidden quotient group**, *and $\nu : G \longrightarrow G/K_\varphi$ is an epimorphism, called the* **hidden epimorphism**. *We will call the above diagram the* **hidden subgroup structure** *of the map $\varphi : G \longrightarrow S$.*

Remark 1. *The underlying intuition motivating this formal definition is as follows: Given a natural surjection (or epimorphism) $\nu : G \longrightarrow G/K_\varphi$, an "archvillain with malice of forethought" hides the algebraic structure of ν by intentionally renaming all the elements of G/K_φ, and "tossing in for good measure" some extra elements to form a set S and a map $\varphi : G \longrightarrow S$.*

The hidden subgroup problem can be stated as follows:

Problem 1 (**Hidden Subgroup Problem (HSP)**)**.** *Given a map*

$$
\varphi : G \longrightarrow S
$$

with hidden subgroup structure, determine a hidden subgroup K_φ of G. An algorithm solving this problem is called a **hidden subgroup algorithm**. *We will call a map with hidden subgroup structure a* **hidden subgroup problem (HSP).**

---

[1]By saying that this diagram is commutative, we mean $\varphi = \iota_\varphi \circ \nu$. This concept generalizes in an obvious way to more complicated diagrams.

The corresponding quantum form of this HSP is stated as follows:

Problem 2 (**Hidden Subgroup Problem: Quantum Version**). *Let*

$$\varphi : G \longrightarrow S$$

be a map with hidden subgroup structure. Construct a quantum implementation of the map φ as follows:

Let $\mathcal{H}_G$ and $\mathcal{H}_S$ be Hilbert spaces defined respectively by the orthonormal bases

$$\{ \, |g\rangle \mid g \in G \, \} \ \ and \ \{ \, |s\rangle \mid s \in S \, \} \ ,$$

and let $s_0 = \varphi(1)$, where 1 denotes the identity of the ambient group G. Finally, let U_φ be a unitary transformation such that

$$U_\varphi : \mathcal{H}_G \otimes \mathcal{H}_S \ \longrightarrow \ \mathcal{H}_G \otimes \mathcal{H}_S$$

$$|g\rangle \, |s_0\rangle \ \longmapsto \ |g\rangle \, |\varphi(g)\rangle \quad ,$$

*Determine the hidden subgroup K_φ with bounded probability of error by making as few queries as possible of the blackbox U_φ. A quantum algorithm solving this problem is called a **quantum hidden subgroup (QHS) algorithm.***

3. The generic QHS algorithm QRand

Let $\varphi : G \longrightarrow S$ be a map from a group G to a set S with hidden subgroup structure. We assume that all representations of G are equivalent to unitary representations[2]. Let $\widehat{G}$ denote a **complete set of distinct irreducible unitary representations** of G. Using multiplicative notation for G, we let 1 denote the **identity** of G, and let s_0 denote its image in S. Finally, let $\widehat{1}$ denote the trivial representation of G.

Remark 2. *If G is abelian, then $\widehat{G}$ becomes the dual group of characters.*

The generic QHS algorithm is given below:

Quantum Subroutine QRand(φ)

Step 0. Initialization

$$|\psi_0\rangle = \left|\widehat{1}\right\rangle |s_0\rangle \in \mathcal{H}_{\widehat{G}} \otimes \mathcal{H}_S$$

Step 1. Application of the inverse Fourier transform $\mathcal{F}_G^{-1}$ of G to the left register

$$|\psi_1\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \, |s_0\rangle \in \mathcal{H}_G \otimes \mathcal{H}_S \ \ ,$$

where $|G|$ denotes the cardinality of the group G.

---

[2]This is true for all finite groups as well as a large class of infinite groups.

Step 2. Application of the unitary transformation U_φ

$$|\psi_2\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \, |\varphi(g)\rangle \in \mathcal{H}_G \otimes \mathcal{H}_S$$

Step 3. Application of the Fourier transform $\mathcal{F}_G$ of G to the left register

$$|\psi_3\rangle = \frac{1}{|G|} \sum_{\gamma \in \widehat{G}} |\gamma| \sum_{g \in G} Trace\left(\gamma(g)^\dagger |\gamma\rangle\right) |\varphi(g)\rangle = \frac{1}{|G|} \sum_{\gamma \in \widehat{G}} |\gamma| \, Trace\left(|\gamma\rangle \, |\Phi\left(\gamma^\dagger\right)\rangle\right) \in \mathcal{H}_{\widehat{G}} \otimes \mathcal{H}_S \ \ ,$$

where $|\gamma|$ denotes the degree of the representation γ, where $\gamma^\dagger$ denotes the contragradient representation (i.e., $\gamma^\dagger(g) = \gamma\left(g^{-1}\right)^T = \overline{\gamma(g)}^T$), where $Trace\left(\gamma^\dagger(g) |\gamma\rangle\right) = \sum_{i=1}^{|\gamma|} \sum_{j=1}^{|\gamma|} \overline{\gamma(g)}_{ji} |\gamma_{ij}\rangle$, and where $\left|\Phi\left(\gamma_{ij}^\dagger\right)\right\rangle = \sum_{g \in G} \overline{\gamma}_{ji}(g) |\varphi(g)\rangle$.

Step 4. Measurement of the left quantum register with respect to the orthonormal basis
$$\left\{ |\gamma_{ij}\rangle \ : \gamma \in \widehat{G}, \ 1 \le i, j \le |\gamma| \right\}.$$
Thus, with probability
$$Prob_\varphi\left(\gamma_{ij}\right) = \frac{|\gamma|^2 \left\langle \Phi\left(\gamma_{ij}^\dagger\right) | \Phi\left(\gamma_{ij}^\dagger\right) \right\rangle}{|G|^2} \ \ ,$$
γ_{ij} is the measured result, and the quantum system "collapses" to the state
$$|\psi_4\rangle = \frac{|\gamma_{ij}\rangle \left|\Phi\left(\gamma_{ij}^\dagger\right)\right\rangle}{\sqrt{\left\langle \Phi\left(\gamma_{ij}^\dagger\right) | \Phi\left(\gamma_{ij}^\dagger\right) \right\rangle}} \in \mathcal{H}_{\widehat{G}} \otimes \mathcal{H}_S$$

Step 5. Output γ_{ij} and stop.

4. Pushing HSPs for the generic QHS algorithm QRand

For certain hidden subgroup problems (HSPs) $\varphi : G \longrightarrow S$, the corresponding generic QHS algorithm QRand either is not physically implementable or is too expensive to implement physically. For example, the HSP φ is usually not physically implementable if the ambient group is infinite (e.g., G is the infinite cyclic group $\mathbb{Z}$), and is too expensive to implement if the ambient group is too large (e.g., G is the symmetric group $\mathbb{S}_{10^{100}}$). In this case, there is a standard generic way of "tweaking" the HSP to get around this problem, which we will call **pushing**.

Definition 2. *Let $\varphi : G \longrightarrow S$ be a map from a group G to a set S. A map $\widetilde{\varphi} : \widetilde{G} \longrightarrow S$ from a group $\widetilde{G}$ to the set S is said to be a **push** of φ, written*
$$\widetilde{\varphi} = Push(\varphi) \ \ ,$$
provided there exists an epimorphism $\mu : G \longrightarrow \widetilde{G}$ from G onto $\widetilde{G}$, and a transversal $\tau : \widetilde{G} \longrightarrow G$ of μ such that $\widetilde{\varphi} = \varphi \circ \tau$.

If the epimorphism μ and the transversal τ are chosen in an appropriate way, then execution of the generic QHS subroutine with input $\widetilde{\varphi} = Push\,(\varphi)$, i.e., execution of

$$QRand\,(\widetilde{\varphi})\quad,$$

will with high probability produce an irreducible representation $\widetilde{\gamma}$ of the group $\widetilde{G}$ which is sufficiently close to an irreducible representation γ of the group G. If this is the case, then there is a polynomial time classical algorithm which upon input $\widetilde{\gamma}$ produces the representation γ.

Obviously, much more can be said about pushing. But unfortunately that would take us far afield from the objectives of this paper. For more information on pushing, we refer the reader to [24].

5. Shor's algorithm

Shor's factoring algorithm is a classic example of a QHS algorithm created from the push of an HSP.

Let N be the integer to be factored. Let $\mathbb{Z}$ denote the additive group of integers, and $\mathbb{Z}_N^\times$ denote the monoid of integers under multiplication modulo N (i.e., the ring of integers modulo N ignoring addition.)

Shor's algorithm is a QHS algorithm that solves the following HSP

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathbb{Z}_N^\times \\ m & \longmapsto & a^m \bmod N \end{array}$$

with unknown hidden subgroup structure given by the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z} & \stackrel{\varphi}{\longrightarrow} & \mathbb{Z}_N^\times \\ {\scriptstyle \nu}\searrow & & \nearrow{\scriptstyle \iota} \\ & \mathbb{Z}/P\mathbb{Z} & \end{array}\quad,$$

where a is an integer relatively prime to N, where P is the hidden integer period of the map $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_N^\times$, where $P\mathbb{Z}$ is the additive subgroup all integer multiples of P (i.e., the hidden subgroup), where $\nu : \mathbb{Z} \longrightarrow \mathbb{Z}/P\mathbb{Z}$ is the natural epimorpism of of the integers onto the quotient group $\mathbb{Z}/P\mathbb{Z}$ (i.e., the hidden epimorphism), and where $\iota : \mathbb{Z}/P\mathbb{Z} \longrightarrow \mathbb{Z}_N^\times$ is the hidden monomorphism.

An obstacle to creating a physically implementable algorithm for this HSP is that the domain $\mathbb{Z}$ of φ is infinite. As observed by Shor, a way to work around this difficulty is to push the HSP.

In particular, as illustrated by the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z} & \stackrel{\varphi}{\longrightarrow} & \mathbb{Z}_N^\times \\ {\scriptstyle \mu}\searrow\nwarrow{\scriptstyle \tau} & & \nearrow{\scriptstyle \varphi = Push\,(\varphi) = \varphi \circ \tau} \\ & \mathbb{Z}_Q & \end{array}\quad,$$

a push $\widetilde{\varphi} = Push\,(\varphi)$ is constructed by selecting the epimorphism $\mu : \mathbb{Z} \longrightarrow \mathbb{Z}_Q$ of $\mathbb{Z}$ onto the finite cyclic group $\mathbb{Z}_Q$ of order Q, where the integer Q is the unique power of 2 such that $N^2 \leq Q < 2N^2$, and choosing the transversal[3]

$$\begin{array}{ccc} \tau : \mathbb{Z}_Q & \longrightarrow & \mathbb{Z} \\ m \bmod Q & \longmapsto & m \end{array} \quad ,$$

where $0 \leq m < Q$.   *This push $\widetilde{\varphi} = Push\,(\varphi)$ is called* **Shor's oracle**.

Shor's algorithm consists in first executing the quantum subroutine $\mathrm{QRAND}(\widetilde{\varphi})$, thereby producing a random character

$$\gamma_{y/Q} : m \bmod Q \mapsto \frac{my}{Q} \bmod 1$$

of the finite cyclic group $\mathbb{Z}_Q$. The transversal τ used in pushing has been engineered to assure that the character $\gamma_{y/Q}$ is sufficiently close to a character

$$\gamma_{d/P} : k \bmod P \mapsto \frac{kd}{P} \bmod 1$$

of the hidden quotient group $\mathbb{Z}/P\mathbb{Z} = \mathbb{Z}_P$. In this case "sufficiently close" means that

$$\left| \frac{y}{Q} - \frac{d}{P} \right| \leq \frac{1}{2P^2} \quad ,$$

which that d/P is a continued fraction convergent of y/Q, and thus can be found found by the classical polynomial time continued fraction algorithm.

6. Description of Grover's algorithm

Now let us turn to Grover's algorithm. We begin with a brief description.

Consider an unstructured database of $N = 2^n$ records labeled without repetitions with the labels
$$0, 1, 2, \ldots, N - 1.$$
We are given the oracle $f : \{0,1\}^n \longrightarrow \{0,1\}$, where

$$f(x) = \begin{cases} 1 & \text{if } j = j_0 \quad (\text{``Yes''}) \\ \\ 0 & \text{otherwise} \quad (\text{``No''}) \end{cases} ,$$

called **Grover's oracle**, and asked to solve the following search problem:

Search Problem for an Unstructured Database. *Find the unknown record labeled as j_0 with the minimum amount of computational work, i.e., with the minimum number of queries of the oracle f, and with bounded probability of error.*

Let $\mathcal{H}$ be the Hilbert space with orthonormal basis

$$|0\rangle, |1\rangle, |2\rangle, \ldots, |N-1\rangle \quad ,$$

---

[3]A **transversal** for an epimorphism $\alpha_\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_Q$ is an injection $\tau_\varphi : \mathbb{Z}_\mathbb{Q} \longrightarrow \mathbb{Z}$ such that $\alpha_\varphi \circ \tau_\varphi$ is the identity map on $\mathbb{Z}_Q$, i.e., a map that takes each element of $\mathbb{Z}_Q$ onto a coset representative of the element in $\mathbb{Z}$.

where $N = 2^n$. Then Grover's oracle is essentially given as the unitary transformation

$$I_{|j_0\rangle} : \quad \mathcal{H} \quad \longrightarrow \quad \mathcal{H}$$
$$|j\rangle \quad \longmapsto \quad (-1)^{f(j)} |j\rangle$$

where

$$I_{|j_0\rangle} = I - 2 |j_0\rangle \langle j_0|$$

is inversion in the hyperplane orthogonal to $|j_0\rangle$.

Let H denote the Hadamard transform on the Hilbert space $\mathcal{H}$. Then Grover's algorithm is given as:

Grover's Algorithm

STEP 0.   (Initialization)

$$|\psi\rangle \longleftarrow H |0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$$

$$k \quad \longleftarrow 0$$

STEP 1.   Loop until $k = \left\lfloor \frac{\pi}{4 \sin^{-1}\left(1/\sqrt{N}\right)} \right\rfloor \approx \left\lfloor \frac{\pi}{4} \sqrt{N} \right\rfloor$

$$|\psi\rangle \longleftarrow Q |\psi\rangle = -H I_{|0\rangle} H I_{|j_0\rangle} |\psi\rangle$$

$$k \quad \longleftarrow k + 1$$

STEP 2.   Measure $|\psi\rangle$ with respect to the standard basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ to obtain the unknown state $|j_0\rangle$ with probability $\geq 1 - \frac{1}{N}$.

---

7. THE SYMMETRY HIDDEN WITHIN GROVER'S ALGORITHM

But where is the *hidden symmetry* in Grover's algorithm ?

Let $\mathbb{S}_N$ be the symmetric group on the symbols

$$0, 1, 2, 3, \ldots, N-1 .$$

Then Grover's algorithm is invariant under the **hidden subgroup**

$$Stab_{j_0} = \{g \in \mathbb{S}_N : g(j_0) = j_0\} \subset \mathbb{S}_N ,$$

called the **stabilizer subgroup** for j_0, i.e., Grover's algorithm is invariant under the group action

$$Stab_{j_0} \times \mathcal{H} \quad \longrightarrow \quad \mathcal{H}$$

$$\left(g, \sum_{j=0}^{N-1} a_j |j\rangle\right) \quad \longmapsto \quad \sum_{j=0}^{N-1} a_j |g(j)\rangle$$

Moreover, if the hidden subgroup $Stab_{j_0}$ is known, then so is the integer j_0, and vice versa.

Thus, Grover's algorithm is an algorithm that solves the following hidden subgroup problem, which we will henceforth refer to as **Grover's hidden subgroup problem**:

GROVER'S HIDDEN SUBGROUP PROBLEM. *Given a map*

$$\mathbb{S}_N \overset{\varphi}{\longrightarrow} S$$

from the the symmetric group $\mathbb{S}_N$ into a target set $S = \{0, 1, 2, \ldots, N-1\}$ with hidden subgroup structure given by the commutative diagram

$$
\begin{array}{ccc}
\mathbb{S}_N & \overset{\varphi}{\longrightarrow} & S \\
{\scriptstyle \nu_{j_0}} \searrow & & \nearrow {\scriptstyle \iota} \\
& \mathbb{S}_N/Stab_{j_0} &
\end{array} \quad ,
$$

where $\nu_{j_0} : S_N \longrightarrow S/Stab_{j_0}$ is the natural surjection of S_N onto the coset space $S/Stab_{j_0}$, and where

$$
\begin{array}{ccc}
\iota : \mathbb{S}_N & \overset{\varphi}{\longrightarrow} & S \\
(j \ j_0)\, Stab_{j_0} & \longmapsto & j
\end{array}
$$

*is the **unknown relabeling** (bijection) of the coset space $S_N/Stab_{j_0}$ onto the set S. Find the hidden subgroup $Stab_{j_0}$ with bounded probability of error.*

Let $(ij) \in \mathbb{S}_N$ denote the permutation that interchanges integers i and j, and leaves all other integers fixed. Thus, (ij) is a transposition if $i \neq j$, and the identity permutation 1 if $i = j$.

Proposition 1. *The set*

$$\{(0j_0), (1j_0), (2j_0), \ldots, ((N-1)j_0)\}$$

is a complete set of distinct coset representatives for the hidden subgroup $Stab_{j_0}$ of $\mathbb{S}_N$, i.e., the coset space $\mathbb{S}_N/Stab_{j_0}$ is given by the following complete set of mutually distinct cosets.

$$\mathbb{S}_N/Stab_{j_0} = \{(0j_0)\, Stab_{j_0}, (1j_0)\, Stab_{j_0}, (2j_0)\, Stab_{j_0}, \ldots, ((N-1)j_0)\, Stab_{j_0}\}$$

Proof. Since

$$(kj_0)\, Stab_{j_0} = (\ell j_0)\, Stab_{j_0} \iff (\ell j_0)^{-1}(kj_0) \in Stab_{j_0} \iff k = l \ ,$$

it follows that

$$(0j_0)\, Stab_{j_0}, (1j_0)\, Stab_{j_0}, (2j_0)\, Stab_{j_0}, \ldots, ((N-1)j_0)\, Stab_{j_0}$$

are mutually distinct cosets of $Stab_{j_0}$ in $\mathbb{S}_N$. It now follows from Lagrange's theorem that the above collection of mutually distinct cosets is complete. $\quad \square$

8. A comparison of Grover's and Shor's algorithms

Now let us compare Shor's algorithm with Grover's.

Let S be the set of integers

$$S = \{0, 1, 2, \ldots, N-1\} \quad,$$

where $N = 2^n$, and let $j_0 \in S$ denote the unknown label to be found by Grover's algorithm.

Shor's algorithm solves the HSP $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_N^{\times}$ with hidden subgroup structure

$$
\begin{array}{ccc}
\mathbb{Z} & \xrightarrow{\ \varphi\ } & \mathbb{Z}_N^{\times} \\
\nu \searrow & & \nearrow \iota \\
& \mathbb{Z}/P\mathbb{Z} &
\end{array} \quad,
$$

where $\mathbb{Z}_N^{\times}$ can be thought of as the result of the unknown ("malicious") relabeling

$$\iota : k + PZ \longmapsto a^k \bmod N$$

of $\mathbb{Z}/P\mathbb{Z}$.

In like manner, Grover's algorithm solves an HSP, namely, the HSP $\varphi : \mathbb{S}_N \longrightarrow S$ with hidden subgroup structure

$$
\begin{array}{ccc}
\mathbb{S}_N & \xrightarrow{\ \varphi\ } & S \\
\nu \searrow & & \nearrow \iota \\
& \mathbb{S}_N/Stab_{j0} &
\end{array} \quad,
$$

where $S = \{0, 1, 2, \ldots, N-1\}$ denotes the set resulting from the unknown ("malicious") relabeling (bijection)

$$\iota : (j\ j_0)\, Stab_{j_0} \longmapsto j$$

of $\mathbb{S}_N/Stab_{j0}$.

For Shor's algorithm, Shor's oracle $\widetilde{\varphi} : \mathbb{Z}_Q \longrightarrow \mathbb{Z}_N^{\times}$ is created by pushing the HSP $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_N^{\times}$ using

$$
\begin{array}{ccc}
\mathbb{Z} & \xrightarrow{\ \varphi\ } & \mathbb{Z}_N^{\times} \\
\mu \searrow \nwarrow \tau & & \nearrow \widetilde{\varphi} \\
& \mathbb{Z}/Q\mathbb{Z} &
\end{array} \quad,
$$

thereby producing $\widetilde{\varphi} = Push(\varphi) = \varphi \circ \tau$ with the transversal $\tau : k \bmod Q \longmapsto k$.

In like manner, for Grover's algorithm, Grover's oracle can be created by pushing the HSP $\varphi : \mathbb{S}_N \longrightarrow S$ using

$$
\begin{array}{ccc}
\mathbb{S}_N & \xrightarrow{\ \varphi\ } & S \\
\mu \searrow \nwarrow \tau & & \nearrow \widetilde{\varphi} \\
& \mathbb{S}_N/Stab_0 &
\end{array} \quad,
$$

thereby producing $\widetilde{\varphi} = Push(\varphi) = \varphi \circ \tau$ with the transversal $\tau : (0\ j)\, Stab_0 \longmapsto \mathbb{S}_N$ of the natural surjection μ.

Although it is not immediately apparent, the resulting push $\widetilde{\varphi}$ (for $j_0 \neq 0$) is actually Grover's oracle relabelled by the injection $\iota : S_N/Stab_{j_0} \longrightarrow S$. For $\widetilde{\varphi} = \varphi \circ \tau = (\iota \circ \nu) \circ \tau = \iota \circ (\nu \circ \tau)$ and

$$(\nu \circ \tau)\left[(0\ j)\,Stab_0\right] = \begin{cases} (0\ j_0)\,Stab_{j_0} & \text{if}\ \ j = j_0 \\ \\ Stab_{j_0} & \text{otherwise} \end{cases}$$

which is informationally the same as Grover's oracle

$$f(j) = \begin{cases} 1 & \text{if}\ \ j = j_0 \\ \\ 0 & \text{otherwise} \end{cases}$$

Hence, we can conclude that Grover's algorithm is an quantum algorithm very much like Shor's algorithm, in that it is a quantum algorithm that solves the Grover hidden subgroup problem.

9. However

However, ... this appears to be where the similarity between these two algorithms ends. For, the standard non-abelian QHS algorithm on $\mathbb{S}_N$ for the HSP φ (or $\widetilde{\varphi}$) can not find the hidden subgroup $Stab_{j_0}$ for each of the following two reasons:

- Since the subgroups $Stab_j$ are not normal subgroups of $\mathbb{S}_N$, it follows from the work of Hallgren et al [11] that the standard non-abelian hidden subgroup algorithm will find the largest normal subgroup of $\mathbb{S}_N$ lying in $Stab_j$. But unfortunately, the largest normal subgroup of $\mathbb{S}_N$ lying in $Stab_j$. is the trivial subgroup of $\mathbb{S}_N$.

- The subgroups $Stab_0$, $Stab_1$, ... , $Stab_{N-1}$ are mutually conjugate subgroups of $\mathbb{S}_N$.

We should also mention that this hidden subgroup approach can not possibly lead to a quantum algorithm that is faster than Grover's.. For Zalka[31] has shown that Grover's algorithm is asymptotically optimal.

A Comparison of Two Quantum Algorithms	
Shor's Algorithm	**Grover's Algorithm**
Similarities	
Shor's algorithm solves an HSP, namely: $$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}_N^{\times} \\ \nu \searrow & & \nearrow \iota \\ & \mathbb{Z}/P\mathbb{Z} & \end{array}$$	Grover's algorithm solves an HSP, namely: $$\begin{array}{ccc} \mathbb{S}_N & \xrightarrow{\varphi} & S \\ \nu \searrow & & \nearrow \iota \\ & \mathbb{S}_N/Stab_{j_0} & \end{array}$$
Pushing φ using $$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}_N^{\times} \\ \mu \searrow \nwarrow \tau & & \nearrow \widetilde{\varphi} \\ & \mathbb{Z}/Q\mathbb{Z} & \end{array}$$ produces $\widetilde{\varphi} = Push(\varphi) = \varphi \circ \tau$ which is Shor's oracle	Pushing φ using $$\begin{array}{ccc} \mathbb{S}_N & \xrightarrow{\varphi} & S \\ \mu \searrow \nwarrow \tau & & \nearrow \widetilde{\varphi} \\ & \mathbb{S}_N/Stab_0 & \end{array}$$ produces $\widetilde{\varphi} = Push(\varphi) = \varphi \circ \tau$ which is Grover's oracle $(j_0 \neq 0)$
Differences	
Repeated calling of the quantum subroutine $\mathrm{QRAND}(\widetilde{\varphi})$ provides enough information to solve the HSP φ	Repeated calling of the quantum subroutine $\mathrm{QRAND}(\widetilde{\varphi})$ provides no information whatsoever about the HSP φ

10. Conclusions and Open Questions

The arguments made in this paper suggest that Grover's and Shor's algorithms are more closely related quantum algorithms than one might at first expect. Although the standard non-abelian QHS algorithm on $\mathbb{S}_N$ can not solve the Grover hidden subgroup problem, there still remains an intriguing question:

Question. *Is there some modification or extension of the stantard non-abelian QHS algorithm on the symmetric group $\mathbb{S}_N$ that actually solves Grover's hidden subgroup problem?*

An answer to the above question could lead to a greater insight into how to create new quantum algorithms.

The methods of this paper can also be applied to Grover's algorithm for multiple marked label search. But can they also be applied to other extensions of Grover's algorithm such as those found in [2], [3]?

References

[1] Bernstein, Ethan, and Umesh Vazirani, **Quantum Complexity Theory**, SIAM J. of Computing, Vol. 26, No. 5, (1997), pp 1411-1473.

[2] Biham, Eli, Ofer Biham, David Biron, Markus Grassl, and Daniel A. Lidar, **Grover's quantum search algorithm for an arbitrary ininitial amplitude distribution**, Phys Rev A 60, (1999), 2742-2745.

[3] Biham, Eli, Ofer Biham, David Biron, Markus Grassl, Daniel A. Lidar, and Daniel Shapira, A**nalysis of generalized Grover's quantum search algorithm using recursion equations**, Phys Rev A 63, 012310 (2001).

[4] Cleve, Richard, Artur Ekert, Chiara Macchiavello, and Michele Mosca, **Quantum Algorithms Revisited**, Phil. Trans. Roy. Soc. Lond., A, (1997). http://xxx.lanl.gov/abs/quant-ph/9708016

[5] Ekert, Artur K.and Richard Jozsa, **Quantum computation and Shor's factoring algorithm**, Rev. Mod. Phys., 68,(1996), pp 733-753.

[6] Ettinger, Mark, and Peter Hoyer, **On Quantum Algorithms for Noncommutative Hidden Subgroups**, (1998). http://xxx.lanl.gov/abs/quant-ph/9807029

[7] Ettinger, Mark, Peter Hoyer, Emanuel Knill, **Hidden Subgroup States Are Almost Orthogonal**, http://xxx.lanl.gov/abs/quant-ph/9901034.

[8] Grover, Lov K., in Proc. 28th Annual ACM Symposium on the Theory of Computation, ACM Press, new York, (1996), 212-219.

[9] Grover, Lov K., **Quantum mechanics helps in searching for a needle in a haystack**, Phys. Rev. Lett., 79(2),(1997). (http://xxx.lanl.gov/abs/quant-ph/9706033)

[10] Grover, Lov K., **A framework for fast quantum mechanical algorithms**, http://xxx.lanl.gov/abs/quant-ph/9711043

[11] Hallgren, Sean, Alexander Russell, Amnon Ta-Shma, **The Hidden subgroup problem and quantum computation using group representations**, Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, Oregon, May 2000, 627-635.

[12] Hallgren, Sean, Alexander Russell, Amnon Ta-Shma, **The Hidden subgroup problem and quantum computation using group representations**, SIAM J. Comput., Vol. 32, No. 4, (2003), 916-934.

[13] Ivanyos, Gabor, Frederic Magniez, and Miklos Santha, **Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem**, (2001). http://xxx.lanl.gov/abs/quant-ph/0102014

[14] Jozsa, Richard, **Quantum algorithms and the Fourier transform**, quant-ph preprint archive 9707033 17 Jul 1997.

[15] Jozsa, Richard, Proc. Roy. Soc. London Soc., Ser. A, 454, (1998), 323 - 337.

[16] Jozsa, Richard, **Quantum factoring, discrete logarithms and the hidden subgroup problem**, IEEE Computing in Science and Engineering, (to appear). http://xxx.lanl.gov/abs/quant-ph/0012084

[17] Kitaev, A., **Quantum measurement and the abelian stabiliser problem,** (1995), quant-ph preprint archive 9511026.

[18] Lomonaco, Samuel J., Jr., **A Rosetta Stone for quantum mechanics with an introduction to quantum computation,** in **"Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium"** PSAPM/58, American Mathematical Society, Providence, RI, (2002). (http://xxx.lanl.gov/abs/quant-ph/0007045)

[19] Lomonaco, Samuel J., Jr., **Shor's quantum factoring algorithm,** PSAPM/58, American Mathematical Society, Providence, RI, (2002), 161-179. (http://xxx.lanl.gov/abs/quant-ph/0010034)

[20] Lomonaco, Samuel J., Jr., **Grover's quantum search algorithm**, PSAPM/58, American Mathematical Society, Providence, RI, (2002), 181-192. (http://arxiv.org/abs/quant-ph/0010040)

[21] Lomonaco, Samuel J., Jr., and Howard E. Brandt, **"Quantum Computation and Information,"** Contemporary Mathematics, Vo. 305, American Mathematical Society, Providence, Rhode Island, (2000).

[22] Lomonaco, Samuel J., Jr., and Louis H. Kauffman, **Quantum hidden subgroup algorithms: A mathematical perspective**, CONM/305, (2000), 139-202. (http://arxiv.org/abs/quant-ph/0201095)

[23] Lomonaco, Samuel J., Jr., **The non-abelian Fourier transform and quantum computation**, MSRI Streaming Video, (2000), http://www.msri.org/publications/ln/msri/2000/qcomputing/lomonaco/1/index.html

[24] Lomonaco, Samuel J., Jr., and Louis H. Kauffman, **Quantum hidden subgroup algorithms on free groups**, (in preparation.)

[25] Mosca, Michelle, and Artur Ekert, **The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer**, Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communication, Springer-Verlag, (to appear). (http://xxx.lanl.gov/abs/quant-ph/9903071)

[26] Russell, Alexander, and Amnon Ta-Shma, **Normal Subgroup Reconstruction and Quantum Computation Using Group Representations**, STOC, (2000).

[27] Shor, Peter W., **Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer**, SIAM J. on Computing, 26(5) (1997), pp 1484 - 1509. (http://xxx.lanl.gov/abs/quant-ph/9508027)

[28] Shor, Peter W., **Introduction to quantum algorithms,** in **"Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium,"** PSAPM/58, American Mathematical Society, Providence, RI, (2002). (http://xxx.lanl.gov/abs/quant-ph/0005003)

[29] van Dam, Wim, and Lawrence Ip, **Quantum Algorithms, for Hidden Coset Problems**, manuscript, http://www.cs.caltech.edu/~hallgren/hcp.pdf

[30] Vazirani, Umesh, **On the power of quantum computation**, Philosophical Tranactions of the Royal Society of London, Series A, 354:1759-1768, August 1998.

[31] Zalka, Christof, **Grover's quantum searching algorithm is optimal**, Phys. Rev. A, Vol. 60, No. 4, (1999), 2746-2751. (http://xxx.lanl.gov/abs/quant-ph/9711070)

University of Maryland Baltimore County (UMBC), Baltimore, MD 21250   USA
E-mail address: Lomonaco@umbc.edu
URL: http://www.csee.umbc.edu/~lomonaco

Current address: University of Illinois at Chicago, Chicago, IL 60607-7045   USA
E-mail address: kauffman@uic.edu
URL: http://www.math.uic.edu/~kauffman