Continuous Quantum Hidden Subgroup Algorithms

Samuel J. Lomonaco, Jr.
Dept. of Comp. Sci. & Electrical Engineering
University of Maryland Baltimore County
Baltimore, MD 21250
Email: Lomonaco@UMBC.EDU
WebPage: http://www.csee.umbc.edu/~lomonaco

Defense Advanced Research Projects Agency (DARPA) & Air Force Research Laboratory, Air Force Materiel Command, USAF Agreement Number F30602-01-2-0522

This work is in collaboration with
Louis H. Kauffman

This work is supported by:
- The National Institute for Standards and Technology (NIST)
- The Mathematical Sciences Research Institute (MSRI).
- L-O-O-P The L-O-O-P Fund.


Hidden Subgroup Algorithms

Def. A Map $\varphi : A \to S$ is said to have hidden subgroup structure if there exist:
- A subgroup $K_p$ of $A$, and
- An injection $t_p : A/K_p \to S$ such that the diagram is commutative.

Hidden Subgroup Structure

Ambient Group $A$ \xrightarrow{\varphi} S \xrightarrow{t_p} S / \tilde{K}_p

Hidden Natural Surjection $A \xrightarrow{\varphi} S \xrightarrow{t_p} A/K_p$
Hidden Subgroup Structure (Cont.)

If $K_\varphi$ is an invariant subgroup of $A$, then

$$H_\varphi = A / K_\varphi$$

is a group, and $\nu: A \to A / K_\varphi$ is an epimorphism.

Origin of QHS Algorithms

Shor’s Quantum factoring algorithm reduces the task of factoring an integer $N$ to the task of finding the period $P$ of a function

$$\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \mod N$$

$$n \mapsto a^n \mod N$$

Kitaev observed that finding the period $P$ is equivalent to finding the subgroup $\mathbb{Z}/\mathbb{Z}$, i.e., the kernel of $\varphi$.

Three Methods for Creating New Quantum Algorithms

Three Ways to create New Quantum Algorithms
• Lifting
• Pushing
• Duality
Hidden Subgroup Algorithms

Some Past Algorithms

- **Wandering Shor**

- **Continuous Shor**

Three Recent QHS Algorithms

- A quantum algorithm on the Circle
- A quantum algorithm dual to Shor’s algorithm
- A highly speculative quantum algorithm for functional integrals

Road Map

- **Shor’s Alg**
  - Lifting
  - QHS Alg on \(\mathbb{Z}\)
  - Duality
  - QHS Alg on \(\mathbb{R} / \mathbb{Z}\)
  - Pushing
  - Dual of Shor’s Alg

- **Lifting & Duality**
  - Lift of Shor Algorithm
  - Dual Lifted Algorithm

Key Idea: Lifting of discrete algorithms to a continuous group
A Lifting of Shor’s Quantum Factoring Algorithm to Integers $\mathbb{Z}$

Fourier Analysis on the Circle

The Circle as a Group

The circle group can be viewed as

- A multiplicative group, i.e., as the unit circle in the complex plane $\mathbb{C}$
  \[ e^{ix} : x \in \mathbb{R} \]
  \[ e^{ix} \cdot e^{iy} = e^{i(x+y)} \]
  where $\mathbb{R}$ denotes the additive group of reals.

A Momentary Digression

The Circle as a Group

The circle group can also be viewed as

- An additive group, i.e., as
  \[ \mathbb{R} / \mathbb{Z} = \text{reals mod 1} \]
  \[ x + y \mod 1 \]
  where $\mathbb{Z}$ denotes the additive group of integers.

The Character Group

The character group $\widehat{A}$ of an abelian group $A$ is defined as

\[ \widehat{A} = \text{Hom}(A, \text{Circle}) = \{ \chi : A \to \text{Circle} : \chi \text{ a morphism} \} \]

with group operation (in multiplicative notation),

\[ (\chi_i \cdot \chi_j)(a) = \chi_i(a) \cdot \chi_j(a) \]

or (in additive notation) as

\[ (\chi_i + \chi_j)(a) = \chi_i(a) + \chi_j(a) \]

The Character Groups of $\mathbb{Z}$ and $\mathbb{R} / \mathbb{Z}$

- The character group of $\mathbb{Z}$ is
  \[ \widehat{\mathbb{Z}} = \{ \chi_n : n \mapsto e^{2\pi i nx} : x \in \mathbb{R} \} = \mathbb{R} / \mathbb{Z} \]

- The character group of $\mathbb{R} / \mathbb{Z}$ is
  \[ \widehat{\mathbb{R} / \mathbb{Z}} = \{ \chi_n : x \mapsto e^{2\pi i nx} : n \in \mathbb{Z} \}
  \equiv \{ \chi_n : x \mapsto nx \mod 1 : n \in \mathbb{Z} \} = \mathbb{Z} \]

$\mathbb{Z} \leftrightarrow \mathbb{R} / \mathbb{Z}$
Fourier Analysis on the Circle $\mathbb{R}/\mathbb{Z}$

The Fourier transform of $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ is defined as the map

$$\hat{f} : \mathbb{Z} \to \mathbb{C}$$

given by

$$\hat{f}(n) = \int dx e^{-inx} f(x)$$

The inverse Fourier transform is defined as

$$f(x) = \sum_{n \in \mathbb{Z}} e^{inx} \hat{f}(n)$$

**Needed Mathematical Machinery**

- Dirac Delta function $\delta(x)$ on $\mathbb{R}/\mathbb{Z}$

- For $P$ a non-zero integer, we will also need on $\mathbb{R}/\mathbb{Z}$ the generalized function

$$\delta_p(x) = \frac{1}{|P|} \sum_{n=0}^{P-1} \delta(x - \frac{n}{P})$$

Rigged Hilbert Space

- $\mathcal{H}_{\mathbb{R}/\mathbb{Z}}$ denotes the rigged Hilbert space on $\mathbb{R}/\mathbb{Z}$ with orthonormal basis

$$\{x : x \in \mathbb{R}/\mathbb{Z}\}, \text{i.e., } (x, y) = \delta(x - y)$$

- The elements of $\mathcal{H}_{\mathbb{R}/\mathbb{Z}}$ are formal integrals of the form

$$\int dx f(x) x$$

Finally, let $\mathcal{H}_{\mathbb{Z}}$ denote the space of formal sums

$$\left\{ \sum_{n=0}^{\infty} a_n |n\rangle : a_n \in \mathbb{C} \quad \forall n \in \mathbb{Z} \right\}$$

with orthonormal basis

$$\{ |n\rangle : n \in \mathbb{Z} \}$$

A Lifting of Shor’s Quantum Factoring Algorithm to Integers $\mathbb{Z}$
Let $\phi : \mathbb{Z} \rightarrow \mathbb{C}$ be a periodic function with hidden minimum period $P$. 

**OBJECTIVE:**

Find $P$

**Step 0. Initialize**

$$\psi_0 = |0\rangle \in \mathcal{H}_2 \otimes \mathcal{H}_C$$

**Step 1. Apply $H \otimes 1$**

$$\psi_1 = \sum_{n \in \mathbb{Z}} e^{2\pi i n} |n\rangle |0\rangle = \sum_{n \in \mathbb{Z}} |n\rangle 0 \in \mathcal{H}_2 \otimes \mathcal{H}_C$$

**Step 2. Apply $U_\phi : |n\rangle |u\rangle \mapsto |n\rangle |u + \phi(n)\rangle$**

$$\psi_2 = \sum_{n \in \mathbb{Z}} |n\rangle |\phi(n)\rangle$$

**Step 3. Apply $\mathcal{Q} \otimes 1$**

$$|\psi\rangle = \frac{1}{\sqrt{P}} \sum_{n \in \mathbb{Z}} e^{i \pi n} |n\rangle$$

**Step 4. Measure**

$$\psi_i = \sum_{n \in \mathbb{Z}} |n\rangle \left\{ \frac{\Omega(n)}{P} \right\}$$

with respect to the observable

$$\mathcal{O} = \int dy \frac{Qy}{Q}$$

to produce a random eigenvalue $m/Q$ and then proceed to find the corresponding $n/P$ using the continued fraction recursion. (We assume $Q \geq 2P^2$)

**The Actual (Un-Lifted) Shor Algorithm**

Make the following approximations by selecting a sufficiently large integer $Q$:

$$Z = Z_0 = \{ k \in \mathbb{Z} : 0 \leq k < P \}$$

$$\mathbb{R}/Z = Z_0 = \left\{ \frac{r}{Q} \mod 1 : r = 0, 1, \ldots, Q - 1 \right\}$$

$\phi : \mathbb{Z} \rightarrow \mathbb{C} = \widetilde{\phi} : Z_0 \rightarrow \mathbb{C}$

$\phi$ is only approximately periodic!

---

**The Actual (Un-Lifted) Shor Algorithm**

The actual (un-lifted) Shor algorithm involves selecting a sufficiently large integer $Q$ and making approximations. The state $|\psi\rangle$ is prepared using periodic functions and measurements are taken to find eigenvalues. The algorithm aims to efficiently factor large integers using quantum computing principles.
Run the algorithm in 
\[ \mathcal{H}_{Z_0} \otimes \mathcal{H}_S \]
and measure the observable
\[ \mathcal{O} \equiv \sum_{r \in \mathbb{Q}} r \left| r \right\rangle \left\langle r \right| \]

A Quantum Hidden Subgroup Algorithm on the Circle

The Dual Algorithm on the Circle

The elements of \( \mathcal{H}_{\mathbb{R}/\mathbb{Z}} \) denote the rigged Hilbert space on \( \mathbb{R}/\mathbb{Z} \) with orthonormal basis
\[ \{x : x \in \mathbb{R}/\mathbb{Z}\} \], i.e., \( \langle x | y \rangle = \delta(x - y) \)

Rigged Hilbert Space

Finally, let \( \mathcal{H}_Z \) denote the space of formal sums
\[ \left\{ \sum_{n=0}^{\infty} a_n |n\rangle : a_n \in \mathbb{C} \quad \forall n \in \mathbb{Z} \right\} \]
with orthonormal basis
\[ \{ |n\rangle : n \in \mathbb{Z}\} \]
Let \( f : \mathbb{R}/\mathbb{Z} \to \mathbb{C} \) be an admissible periodic function of minimum rational period \( \alpha \in \mathbb{Q}/\mathbb{Z} \).

**Proposition:** Let \( \alpha = a_1/a_2 \) (with \( \gcd(a_1, a_2) = 1 \)) be a period of \( f \). Then \( 1/a_2 \) is also a period of \( f \).

**Remark:** Hence, the minimum rational period is always the reciprocal of an integer modulo 1.

**Step 0. Initialize**

\[ \psi_0 = 0 \in \mathcal{H}_\mathbb{R} \otimes \mathcal{H}_\mathbb{C} \]

**Step 1. Apply \( \mathcal{F}^{-1} \otimes 1 \)**

\[ \psi_1 = \int_0^1 dx e^{2\pi i nx} \phi(x) = 0 = \psi_0 \in \mathcal{H}_\mathbb{R} \otimes \mathcal{H}_\mathbb{C} \]

**Step 2. Apply**

\[ U_\phi : x \mapsto x + \phi(x) \]

\[ \psi_z = \int_0^1 dx \phi(x) \]

**Letting** \( x_m = x - \frac{m}{a} \), we have

\[ \int dx e^{-2\pi i m x} \phi(x) = \sum_{n=0}^{a-1} \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n=0}^{a-1} \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \left( \sum_{n=0}^{a-1} e^{2\pi i n \delta} \right) \int dx e^{-2\pi i m x} \phi(x) \]

\[ = \left( \sum_{n=0}^{a-1} e^{2\pi i n \delta} \right) \int dx e^{-2\pi i m x} \phi(x) \]

But \[ \sum_{n=0}^{a-1} e^{2\pi i n \delta} = a \delta_{n=0} + \left\{ \begin{array}{ll} a & \text{if } n = 0 \mod a \\ 0 & \text{otherwise} \end{array} \right. \]

Thus,

\[ \psi_3 = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

**Step 3. Apply \( \mathcal{F} \otimes 1 \)**

\[ \psi_3 = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

But \[ \sum_{n=0}^{a-1} e^{2\pi i n \delta} = a \delta_{n=0} + \left\{ \begin{array}{ll} a & \text{if } n = 0 \mod a \\ 0 & \text{otherwise} \end{array} \right. \]

Thus,

\[ \psi_3 = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

\[ = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

**Step 4. Measure**

\[ \psi_3 = \sum_{n \in \mathbb{Z}} \langle \ell a | \Omega (\ell a) \rangle \]

with respect to the observable

\[ \mathcal{O} = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi i n x} \phi(x) \]

to produce a random eigenvalue \( \ell a \).
The corresponding discrete algorithm

The Algorithmic Dual of Shor’s Quantum Factoring Algorithm

We now create a corresponding discrete algorithm

The approximations are:

\[ Z = \mathbb{Z}_Q = \{ k \in \mathbb{Z} : 0 \leq k < P \} \]
\[ R / Z = \mathbb{Z}_Q = \left\{ \frac{r}{Q} \mod 1 : r = 0, 1, \ldots, Q-1 \right\} \]

\[ \varphi : \mathbb{Z} \rightarrow \mathbb{C} = \widetilde{\varphi} : \mathbb{Z}_Q \rightarrow \mathbb{C} \]

\[ \varphi \] is only approximately periodic!

Run the algorithm in

\[ \mathcal{H}_{\mathbb{Z}_Q} \otimes \mathcal{H}_S \]

and measure the observable

\[ \mathcal{O} = \sum_{k=0}^{Q-1} k |k\rangle \langle k| \]

Quantum Algorithms based on Feynman Functional integrals

Caveat Emptor

The following algorithm is highly speculative.

In the spirit of Feynman, the following quantum algorithm is based on functional integrals whose existence is difficult to determine, let alone approximate.
The Space Paths

Paths = all continuous paths \( x: [0,1] \rightarrow \mathbb{R}^n \) which are \( L^1 \) with respect to the inner product

\[ x \cdot y = \int_0^1 ds \, x(s) y(s) \]

Paths is a vector space over \( \mathbb{R} \) with respect to

\[
\begin{align*}
(\lambda x)(s) &= \lambda x(s) \\
(x + y)(s) &= x(s) + y(s)
\end{align*}
\]

The Problem to be Solved

Let \( \varphi: \text{Paths} \rightarrow \mathbb{C} \) be a functional with a hidden subspace \( V \) of Paths such that

\[ \varphi(x + v) = \varphi(x) \quad \forall v \in V \]

Objective. Create a quantum algorithm that finds the hidden subspace \( V \).

The Ambient Rigged Hilbert Space

Let \( \mathcal{H}_{\text{Paths}} \) be the rigged Hilbert space with orthonormal basis,

\[ \{ |x\rangle : x \in \text{Paths} \} \]

and with bracket product

\[ \langle x | y \rangle = \delta(x - y) \]

Parenthetical Remark

Please note that \( \text{Paths} \) can be written as the following disjoint union:

\[ \text{Paths} = \bigcup_{v \in V'} (v + V') \]

Step 0. Initialize

\[ |\psi_0\rangle = 0 \otimes 0 \in \mathcal{H}_{\text{Paths}} \otimes \mathcal{H}_C \]

Step 1. Apply \( \pi' \otimes 1 \)

\[ |\psi_1\rangle = \int_{\text{Paths}} Dx \, e^{2\pi i \xi_0} |x\rangle \otimes |0\rangle = \int_{\text{Paths}} Dx \, |x\rangle \otimes |0\rangle \]

Step 2. Apply \( U_\varphi : |x\rangle \mapsto |x\rangle \otimes |x + \varphi(x)\rangle \)

\[ |\psi_2\rangle = \int_{\text{Paths}} Dx \, |x\rangle \otimes |\varphi(x)\rangle \]

Step 3. Apply \( \pi \otimes 1 \)

\[ |\psi_3\rangle = \int_{\text{Paths}} Dy \int_{\text{Paths}} Dx \, e^{2\pi i \xi y} |y\rangle \langle x + \varphi(x)\rangle = \int_{\text{Paths}} Dy |y\rangle \int_{\text{Paths}} Dx \, e^{2\pi i \xi y} \langle x + \varphi(x)\rangle = \int_{\text{Paths}} Dy |y\rangle \int_{\text{Paths}} Dx \, e^{2\pi i \xi y} \langle x \rangle \]
But
\[ \int_{\text{Paths}} Dv e^{2\pi i y} \phi(x) = \int \int Dv e^{2\pi i y} \phi(x) \]
\[ = \int Dv \int Dv e^{2\pi i (v+x)} \phi(v+x) \]
\[ = \int Dv e^{2\pi i y} \int Dv e^{2\pi i x} \phi(x) \]

However,
\[ \int_{\text{Paths}} Dv e^{2\pi i y} = \int_{\text{Paths}} Du \delta(y-u) \]

So,
\[ | \psi_s \rangle = \int_{\text{Paths}} Dy | \psi_0 \rangle \int_{\text{Paths}} Dv e^{2\pi i y} \int_{\text{Paths}} Dv e^{2\pi i x} \phi(x) \]
\[ = \int_{\text{Paths}} Dy \int_{\text{Paths}} Du \delta(y-u) \int_{\text{Paths}} Dv e^{2\pi i x} \phi(x) \]
\[ = \int_{\text{Paths}} Du | \psi \rangle \int_{\text{Paths}} Dv e^{2\pi i x} \phi(x) \]
\[ = \int_{\text{Paths}} Du | \Omega(u) \rangle \]

**Step 4. Measure**

\[ | \psi_s \rangle = \int_{\text{Paths}} Dv u | \Omega(u) \rangle \]

with respect to the observable

\[ A = \int_{\text{Paths}} Dw w | w \rangle \langle w | \]

to produce a random element of \( V \perp \)

**Question**

Can the above path integral quantum algorithm be modified in such a way as to create a quantum algorithm for the Jones polynomial? I.e., can it be modified by replacing \( \text{Paths} \) by the space of gauge connections, and by making suitable modifications?

\[ \tilde{\psi}(K) = \int DA \psi(A) \mathcal{U}_K(A) \]

where \( \mathcal{U}_K(A) \) is the Wilson loop

\[ \mathcal{U}_K(A) = \text{tr} \left( P \exp \left( \oint K x A \right) \right) \]
