Overview

Four Talks

- A Rosetta Stone for Quantum Computation
- Three Quantum Algorithms
- Quantum Hidden Subgroup Algorithms
- An Entangled Tale of Quantum Entanglement

Continuous Quantum Hidden Subgroup Algorithms

This work is supported by:

- The National Institute for Standards and Technology (NIST)
- The Mathematical Sciences Research Institute (MSRI).
- The L-O-O-P Fund.

This work is in collaboration with
Louis H. Kauffman
**Existing Quantum Algorithms**

- Hidden Subgroup Algorithms - Shor-Like Algorithms
- Amplitude amplification - Grover-Like Algorithms
- Quantum Algorithms Simulating Quantum Systems
- Sipser’s Algorithm
- Adiabatic Algorithms

**Some Existing HSA’s**

- Hidden subgroup algorithms
  - Deutsch-Jozsa
  - Simon
  - Shor
  - Legendre symbol
  - Hallgen
  - Various Non-abel. Algorithms
  - Others

We will now discuss the following Six HSA’s

- Continuous Shor on \( \mathbb{R} \)
- Wandering Shor
- Lift of Shor to \( \mathbb{Z} \)
- HSA on Circle
- Dual Shor HSA
- HSA for Functional Integrals

These Six Algorithms Can Be Found in the Following Three Papers


**Hidden Subgroup Algorithms**

Def. A Map \( \varphi : A \rightarrow S \) is said to have hidden subgroup structure if there exist

- A subgroup \( K \) of \( A \), and
- An injection \( t_p : A/K \rightarrow S \)

s. t. the diagram

\[
\begin{array}{ccc}
A & \xrightarrow{\varphi} & S \\
\downarrow A & & \uparrow t_p \\
A/K & & S \\
\end{array}
\]

is commutative.
Hidden Subgroup Structure (Cont.)

If $K_\varphi$ is an invariant subgroup of $A$, then $H_\varphi = A/K_\varphi$ is a group, and $\varphi: A \to A/K_\varphi$ is an epimorphism.

Quantum Hidden Subgroup Algorithms

<table>
<thead>
<tr>
<th>Quantum Algorithm</th>
<th>Ambient Gp</th>
<th>Hidden Subgp $K_\varphi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsch-Jozsa</td>
<td>$Z_2$</td>
<td>$\kappa = {0}/Z_2$</td>
</tr>
<tr>
<td>Simon</td>
<td>$Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$</td>
<td>$K_\varphi \cong Z_2$</td>
</tr>
<tr>
<td>Shor Factoring</td>
<td>$\mathbb{Z}$</td>
<td>$K_\varphi = P\mathbb{Z}$</td>
</tr>
</tbody>
</table>

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

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

The Hidden Subgroup Problem (HSP)

Given a map $\varphi: A \to S$ with hidden subgroup structure, determine the hidden subgroup $K_\varphi$ of the ambient group $A$. An algorithm solving this problem is called a hidden subgroup algorithm (HSA).

The First of the Three Papers


The Quantum Hidden Subgroup Paper

Shows how to create a

Meta Algorithm

\[ A \xrightarrow{\varphi} S \xrightarrow{\text{Meta Algorithm}} \text{Alg}_\varphi \]
An Analogy

• Autos before Henry Ford

• Autos after Henry Ford

Three Methods for Creating New Quantum Algorithms

• Lifting

• Pushing

• Duality

Summary

3 Ways to create New Quantum Algorithms

• Lifting

• Pushing

• Duality
Hidden Subgroup Algorithms

Some Past Algorithms

- Wandering Shor

- Continuous Shor

Wandering Shor

\[ \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\phi} S \]

Shor Trans.\[ i \uparrow \downarrow \nu \quad \phi = \phi \circ \iota \]

Phase Approx Gp Approx Set

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
  \[ \rightarrow \] Quantum algorithm for the Jones polynomial

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
- QHS Algorithms for Functional Integrals
- Dual Lifted Algorithm
- Dual Shor Algorithm
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 $\mathbb{C}$
  $$\{e^{i\pi x} : x \in \mathbb{R}\}$$
  $$e^{i\pi x} \cdot e^{i\pi y} = e^{i\pi (x+y)}$$
  where $\mathbb{R}$ denotes the additive group of reals.

The Circle as a Group

The circle group can also be viewed as

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

The Character Group

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

$$\hat{A} = \text{Hom}(A, \text{Circle}) = \{\chi : A \to \text{Circle} : \chi \text{ a morphism}\}$$

with group operation (in multiplicative notation),

$$(\chi_1 \cdot \chi_2)(a) = \chi_1(a) \cdot \chi_2(a)$$

or (in additive notation) as

$$(\chi_1 + \chi_2)(a) = \chi_1(a) + \chi_2(a)$$

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

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

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

$\mathbb{Z} \leftrightarrow \mathbb{R}/\mathbb{Z}$

Discrete $\rightarrow$ Continuous
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

$$\hat{f}(n) = \int dx e^{-2\pi i nx} f(x).$$

The inverse Fourier transform is defined as

$$f(x) = \sum_{n \in \mathbb{Z}} e^{2\pi i nx} \hat{f}(n).$$

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

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

Rigged Hilbert Space

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

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

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

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

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

$$\sum_{n=-\infty}^{\infty} a_n |n\rangle : a_n \in \mathbb{C} \ \forall n \in \mathbb{Z}\}$$

with orthonormal basis

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

A Lifting of Shor's Quantum Factoring Algorithm to Integers $\mathbb{Z}$

Lifting & Duality

Lift of Shor Algorithm

Shor Algorithm
Let \( \varphi : \mathbb{Z} \to \mathbb{C} \) be periodic function with hidden minimum period \( P \).

OBJECTIVE: Find \( P \)

- Step 0. Initialize
  \[ \psi_0 = 0, 0 \in \mathcal{H}_{\mathbb{Z}/P} \otimes \mathcal{H}_C \]

- Step 1. Apply \( \mathcal{J} \otimes 1 \)
  \[ \psi_1 = \sum_{n \in \mathbb{Z}} e^{2\pi i n} \psi(0) \in \mathcal{H}_{\mathbb{Z}/P} \otimes \mathcal{H}_C \]

- Step 2. Apply \( U_\psi : |n, u \rangle \mapsto |n, u + \varphi(n) \rangle \)
  \[ \psi_2 = \sum_{n \in \mathbb{Z}} n \otimes \varphi(n) \]

- Step 3. Apply \( \mathcal{J} \otimes 1 \)
  \[
  \begin{align*}
  \psi_3 &= \int dx \left( \sum_{n \in \mathbb{N}} e^{2\pi i n} \varphi(n) \right) \\
  &= \int dx \left( \sum_{n \in \mathbb{N}} \sum_{r \in \mathbb{Z}} e^{2\pi i (n+r)} \varphi(n) \right) \\
  &= \int dx \left( \sum_{n \in \mathbb{N}} \sum_{r \in \mathbb{Z}} e^{2\pi i n} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right) \\
  &= \sum_{n \in \mathbb{N}} \int dx \delta(x) \left( \sum_{r \in \mathbb{Z}} e^{2\pi i r} \varphi(n) \right)
  \end{align*}
\]

- Step 4. Measure
  \[
  \psi_4 = \sum_{n \in \mathbb{N}} n \otimes \varphi(n) \otimes \Omega(n/n_P) \\
  \]

with respect to the observable
  \[ \mathcal{O} = \int dy \frac{Q y}{Q} |y\rangle \langle y| \]

and then proceed to find the corresponding \( n/P \) using the continued fraction recursion. \( (\text{We assume } Q \geq 2P^2) \)

The Actual (Un-Lifted) Shor Algorithm

Make the following approximations by selecting a sufficiently large integer \( Q \) :

\[ Z = \mathbb{Z}_0 = \{ k \in \mathbb{Z} : 0 \leq k < Q \} \]
\[ \mathbb{R}/\mathbb{Z} = \mathbb{Z}_0 = \left\{ \frac{r}{Q} \right\} \mod 1 : r = 0, 1, \ldots, Q - 1 \]
\[ \varphi : \mathbb{Z} \to \mathbb{C} \approx \tilde{\varphi} : \mathbb{Z}_0 \to \mathbb{C} \]
\[ \tilde{\varphi} \text{ is only approximately periodic!} \]
Run the algorithm in \( \mathcal{H}_{\mathbb{Z}_0} \otimes \mathcal{H}_S \) and measure the observable
\[
C = \sum_{r=0}^{Q-1} Q^{-1} \sum_{\alpha=0}^{Q-1} |Q^{-1} \alpha + r\rangle \langle Q^{-1} \alpha + r|.
\]

**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., \( \langle x|y\rangle = \delta(x-y) \).

The elements of \( \mathcal{H}_{\mathbb{R}/\mathbb{Z}} \) are formal integrals of the form
\[
\int dx f(x) |x\rangle.
\]

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

**Proposition:**

Let \( \alpha = a_1 / a_2 \) (with \( \text{gcd}(a_1, a_2) = 1 \)) 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**

\[ \psi_0 = 0, 0 \in \mathbb{H}_a \otimes \mathbb{H}_c \]

**Step 1. Apply** \( \varphi^1 \otimes 1 \)

\[ \psi_1 = \int dx e^{\varphi(x)} \big| 0 = \int dx \cdot 0 \in \mathbb{H}_a \otimes \mathbb{H}_c \]

**Step 2. Apply** \( \mathcal{U}_\varphi : x \mapsto x + \varphi(x) \)

\[ \psi_2 = \int dx \varphi(x) \]

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

\[ \int dx e^{-2\pi in} \varphi(x) = \sum_{\text{mod } a} \left[ \int dx e^{-2\pi in} \varphi(x) \right] = \sum_{\text{mod } a} \left[ \int dx e^{-2\pi i s_n x} \varphi(x) \right] \]

But \( \sum_{\text{mod } a} \frac{e^{-2\pi in}}{a} = a \delta_{n \equiv 0 \text{mod } a} \) if \( n \equiv 0 \text{mod } a \), otherwise

Thus,

\[ \psi_3 = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi in} \varphi(x) = \sum_{n \in \mathbb{Z}} n \int dx e^{-2\pi in} \varphi(x) = \sum_{n \in \mathbb{Z}} n \varphi(n) = \sum_{n \in \mathbb{Z}} \Omega(\alpha) a \]

**Step 4. Measure**

\[ \psi_4 = \sum_{n \in \mathbb{Z}} \frac{\ell a}{\Omega(\ell a)} \]

with respect to the observable

\[ \ell = \sum_{n \in \mathbb{Z}} n \frac{n}{n} \]

to produce a random eigenvalue \( \ell a \).
The

The Algorithmic Dual

of

Shor's Quantum

Factoring Algorithm

The corresponding discrete
algorithm

We now create a corresponding
discrete algorithm

The approximations are:

\[ Z \approx \{ k \in \mathbb{Z} : 0 \leq k < P \} \]

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

\[ \varphi : \mathbb{Z} \rightarrow \mathbb{C} \approx \bar{\varphi} : \mathbb{Z}_0 \rightarrow \mathbb{C} \]

\( \varphi \) is only approximately periodic!

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.

Run the algorithm in

\[ \mathcal{H}_{\mathbb{Z}_0} \otimes \mathcal{H}_S \]

and measure the observable

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

Paths = all continuous paths \( x : [0,1] \to \mathbb{R}^n \) which are \( L^2 \) with respect to the inner product

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

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

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

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:

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

Step 0. Initialize

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

Step 1. Apply \( \varphi \otimes 1 \)

\[
|\psi_1\rangle = \int \mathcal{D}x \, e^{\text{ix}\psi_0} |x\rangle |0\rangle = \int \mathcal{D}x \, |x\rangle |0\rangle
\]

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

\[
|\psi_2\rangle = \int \mathcal{D}x \, |x\rangle |\varphi(x)\rangle
\]

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

\[
|\psi_3\rangle = \int \mathcal{D}y \int \mathcal{D}x \, e^{-\text{ix} \varphi(y)} |y\rangle |\varphi(x)\rangle
\]

\[
= \int \mathcal{D}y \, |y\rangle \int \mathcal{D}x \, e^{-\text{ix} \varphi(|y\rangle)} |\varphi(x)\rangle
\]
But

\[
\int Path \, D x e^{2\pi i x y} \varphi(x) = \int \int Path \, D x e^{2\pi i x y} \varphi(x)
\]

\[
= \int \int Path \, D x e^{2\pi i (v+x) y} \varphi(v+x)
\]

\[
= \int \int Path \, D x e^{2\pi i x y} \varphi(x)
\]

However,

\[
\int Path \, D x e^{2\pi i x y} = \int Path \, D x \delta(y-u)
\]

So,

\[
|\psi_3\rangle = \int Path \, D y \int Path \, D x e^{2\pi i x y} \int Path \, D x e^{-2\pi i x y} \varphi(x)
\]

\[
= \int Path \, D y \int Path \, D u \delta(y-u) \int Path \, D x e^{-2\pi i x y} \varphi(x)
\]

\[
= \int Path \, D u \int Path \, D x e^{-2\pi i x y} \varphi(x)
\]

\[
= \int Path \, D u \Omega(u)
\]

*Step 4. Measure

\[
|\psi_3\rangle = \int \int Path \, D w w \varphi |w\rangle
\]

with respect to the observable

\[A = \int Path \, D w w |w\rangle \langle w|\]

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 Paths by the space of gauge connections, and by making suitable modifications?

\[\psi(K) = \int \int \int Path \, D A \psi(A) \mathcal{A}_k(A)\]

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

\[\mathcal{A}_k(A) = \text{tr} \left( P \exp \left( \oint_A A \right) \right)\]

Quantum Computation and Information, Samuel J. Lomonaco, Jr. and Howard E. Brandt (editors), AMS CONM/305, (2002).