

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

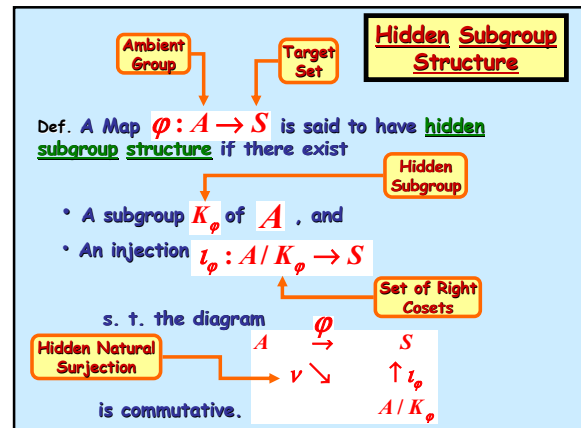
This work is supported by:

-  The Defense Advance Research Projects Agency (DARPA) & Air Force Research Laboratory (AFRL), Air Force Materiel Command, USAF Agreement Number F30602-01-2-0522.
-  The National Institute for Standards and Technology (NIST)
-  The Mathematical Sciences Research Institute (MSRI).
-  The L-O-O-P Fund.

• Kauffman & Lomonaco, Entanglement Criteria - Quantum and Topological, <http://xxx.lanl.gov/abs/quant-ph/0304091>

• Lomonaco & Kauffman, Continuous Quantum Hidden Subgroup Algorithms, <http://xxx.lanl.gov/abs/quant-ph/0304084>

Hidden Subgroup Algorithms



Hidden Subgroup Structure (Cont.)

If K_φ is an invariant subgroup of A , then $H_\varphi = A / K_\varphi$ is a group, and $v: A \rightarrow A / K_\varphi$ 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

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

$$n \mapsto a^n \bmod N$$

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

Three Methods for Creating New Quantum Algorithms

Two Ways to Create New Quantum Algorithms
Lifting and Pushing

Given $\varphi: A \rightarrow S$

A 3rd Way to Create New Quantum Algorithms
Duality

Summary
3 Ways to create New Quantum Algorithms

- Lifting
- Pushing
- Duality

Hidden Subgroup Algorithms

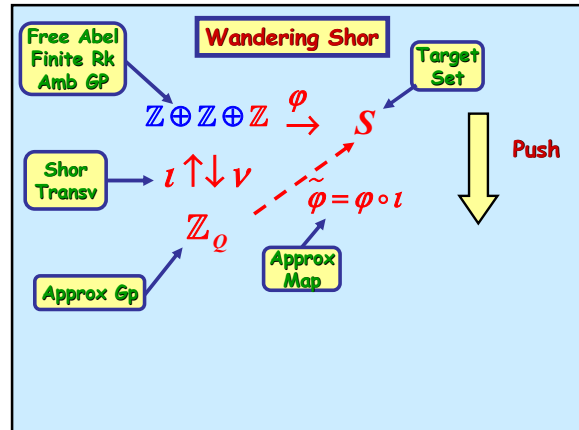
Some Past Algorithms

• **Wandering Shor**

• Lomonaco & Kauffman, **Quantum Hidden Subgroup Algorithms: A Mathematical Perspective**, AMS, CONM/305, (2002).
<http://xxx.lanl.gov/abs/quant-ph/0201095>

• **Continuous Shor**

• Lomonaco & Kauffman, **A Continuous Variable Shor Algorithm**,
<http://xxx.lanl.gov/abs/quant-ph/0210141>



Continuous Shor

Ambient Group
Add. Gp of Reals

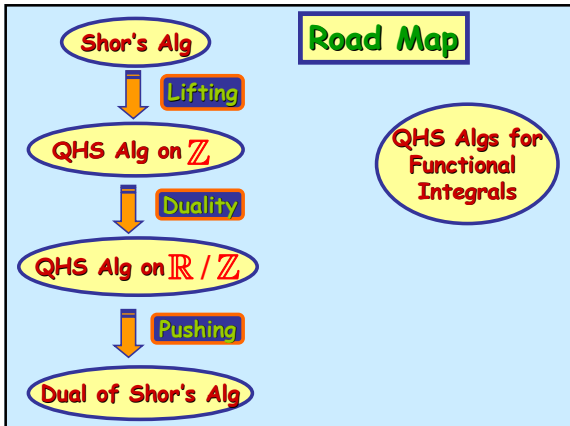
$$\mathbb{R} \xrightarrow{\varphi} S$$

Key Idea: Lifting of discrete algorithms to a continuous groups

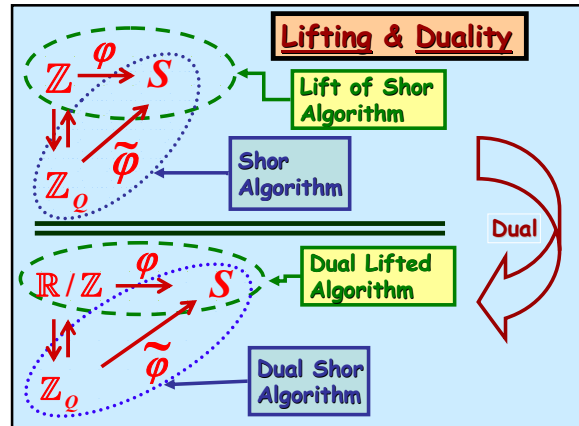
Three Recent QHS Algorithms

- 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



Lifting & Duality



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

A Momentary Digression

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}

$$\{e^{2\pi i x} : x \in \mathbb{R}\}$$

$$e^{2\pi i x} \cdot e^{2\pi i y} = e^{2\pi i(x+y)}$$

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

$$\mathbb{R} / \mathbb{Z} = \text{reals mod } 1$$

$$x + y \text{ mod } 1$$

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

$$\widehat{A} = \text{Hom}(A, \text{Circle})$$

$$= \{\chi : A \rightarrow \text{Circle} : \chi \text{ a morphism}\}$$

with group operation (in multiplicative notation),

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

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

$$\widehat{\mathbb{Z}} = \{\chi_x : n \mapsto e^{2\pi i n x} : x \in \mathbb{R}\} = \mathbb{R} / \mathbb{Z}$$

- The character group of \mathbb{R} / \mathbb{Z} is

$$\widehat{\mathbb{R} / \mathbb{Z}} \cong \{\chi_n : x \mapsto e^{2\pi i n x} : n \in \mathbb{Z}\}$$

$$\cong \{\chi_n : x \mapsto nx \text{ mod } 1 : n \in \mathbb{Z}\} = \mathbb{Z}$$

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

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

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

$$\widehat{f}: \mathbb{Z} \rightarrow \mathbb{C}$$

given by

$$\widehat{f}(n) = \oint dx e^{-2\pi i n x} f(x)$$

The *inverse Fourier transform* is defined as

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

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

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

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

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

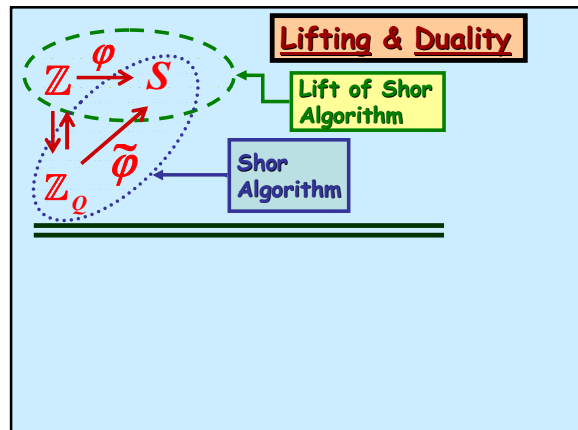
Finally, let $\mathcal{H}_{\mathbb{Z}}$ denote the space of formal sums

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

with orthonormal basis

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

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



Periodic Functions on \mathbb{Z}

Let $\varphi: \mathbb{Z} \rightarrow \mathbb{C}$ be periodic function with hidden minimum period P .

OBJECTIVE:

Find P

- Step 0. Initialize

$$|\psi_0\rangle = |0\rangle|0\rangle \in \mathcal{H}_{\mathbb{R}/\mathbb{Z}} \otimes \mathcal{H}_{\mathbb{C}}$$

- Step 1. Apply $\mathcal{F}^{-1} \otimes \mathbf{1}$

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

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

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

- Step 3. Apply $\mathcal{F} \otimes \mathbf{1}$

$$\begin{aligned} |\psi_3\rangle &= \int dx |x\rangle \sum_{n \in \mathbb{Z}} e^{-2\pi i n x} |\varphi(n)\rangle \in \mathcal{H}_{\mathbb{R}/\mathbb{Z}} \otimes \mathcal{H}_{\mathbb{C}} \\ &= \int dx |x\rangle \sum_{n_1 \in \mathbb{Z}} \sum_{n_0=0}^{P-1} e^{-2\pi i (n_1 P + n_0) x} |\varphi(n_1 P + n_0)\rangle \\ &= \int dx |x\rangle \left(\sum_{n_1 \in \mathbb{Z}} e^{-2\pi i n_1 P x} \right) \sum_{n_0=0}^{P-1} e^{-2\pi i n_0 x} |\varphi(n_0)\rangle \\ &= \int dx |x\rangle \delta_P(x) \sum_{n_0=0}^{P-1} e^{-2\pi i n_0 x} |\varphi(n_0)\rangle \\ &= \sum_{n=0}^{P-1} \frac{n}{P} \left(\frac{1}{P} \sum_{n_0=0}^{P-1} e^{-2\pi i n_0 x} |\varphi(n_0)\rangle \right) \\ &= \sum_{n=0}^{P-1} \frac{n}{P} \left| \Omega\left(\frac{n}{P}\right) \right\rangle \end{aligned}$$

- Step 4. Measure

$$|\psi_3\rangle = \sum_{n=0}^{P-1} \frac{n}{P} \left| \Omega\left(\frac{n}{P}\right) \right\rangle$$

with respect to the observable

$$\mathcal{O} = \int dy \lfloor \frac{Qy}{P} \rfloor |y\rangle\langle y|$$

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

The Actual (Un-Lifted) Shor Algorithm

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

$$\mathbb{Z} \approx \mathbb{Z}_Q = \{k \in \mathbb{Z} : 0 \leq k < Q\}$$

$$\mathbb{R}/\mathbb{Z} \approx \mathbb{Z}_Q = \left\{ \frac{r}{Q} \bmod 1 : r = 0, 1, \dots, Q-1 \right\}$$

$$\varphi: \mathbb{Z} \rightarrow \mathbb{C} \approx \tilde{\varphi}: \mathbb{Z}_Q \rightarrow \mathbb{C}$$

$\tilde{\varphi}$ is only approximately periodic!

Run the algorithm in

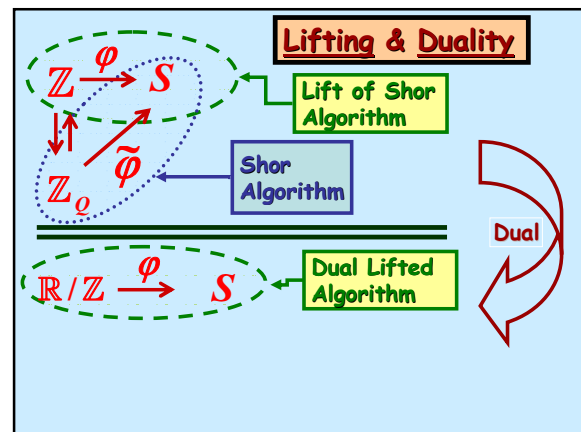
$$\mathcal{H}_{\mathbb{Z}_Q} \otimes \mathcal{H}_S$$

and measure the observable

$$\mathcal{O} = \sum_{r=0}^{Q-1} \frac{r}{Q} \left| \frac{r}{Q} \right\rangle \left\langle \frac{r}{Q} \right|$$

A Quantum Hidden Subgroup Algorithm on the Circle

The Dual Algorithm on the Circle



Rigged Hilbert Space

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

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

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

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

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

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

with orthonormal basis

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

Periodic Admissible Functions on \mathbb{R}/\mathbb{Z}

Let $f: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{C}$ 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

$$|\psi_0\rangle = |0\rangle|0\rangle \in \mathcal{H}_{\mathbb{Z}} \otimes \mathcal{H}_{\mathbb{C}}$$

• Step 1. Apply $\mathcal{F}^{-1} \otimes 1$

$$|\psi_1\rangle = \oint dx e^{2\pi i x \cdot 0} |x\rangle|0\rangle = \oint dx |x\rangle|0\rangle \in \mathcal{H}_{\mathbb{R}/\mathbb{Z}} \otimes \mathcal{H}_{\mathbb{C}}$$

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

$$|\psi_2\rangle = \oint dx |x\rangle|\varphi(x)\rangle$$

• Step 3. Apply $\mathcal{F} \otimes 1$

$$\begin{aligned} |\psi_3\rangle &= \sum_{n \in \mathbb{Z}} \oint dx e^{-2\pi i n x} |n\rangle|\varphi(x)\rangle \\ &= \sum_{n \in \mathbb{Z}} |n\rangle \oint dx e^{-2\pi i n x} |\varphi(x)\rangle \in \mathcal{H}_{\mathbb{Z}} \otimes \mathcal{H}_{\mathbb{C}} \end{aligned}$$

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

$$\begin{aligned} \oint dx e^{-2\pi i n x} |\varphi(x)\rangle &= \sum_{m=0}^{a-1} \int_{\frac{m}{a}}^{\frac{m+1}{a}} dx e^{-2\pi i n x} |\varphi(x)\rangle \\ &= \sum_{m=0}^{a-1} \int_0^{\frac{1}{a}} dx_m e^{-2\pi i n (x_m + \frac{m}{a})} \left| \varphi\left(x_m + \frac{m}{a}\right) \right\rangle \\ &= \left(\sum_{m=0}^{a-1} e^{-\frac{2\pi i n m}{a}} \right) \int_0^{\frac{1}{a}} dx e^{-2\pi i n x} |\varphi(x)\rangle \end{aligned}$$

But $\sum_{m=0}^{a-1} e^{-\frac{2\pi i n m}{a}} = a \delta_{n=0 \bmod a} = \begin{cases} a & \text{if } n = 0 \bmod a \\ 0 & \text{otherwise} \end{cases}$

Thus,

$$\begin{aligned} |\psi_3\rangle &= \sum_{n \in \mathbb{Z}} |n\rangle \oint dx e^{-2\pi i n x} |\varphi(x)\rangle \\ &= \sum_{n \in \mathbb{Z}} |n\rangle \delta_{n=0 \bmod a} \int_0^{\frac{1}{a}} dx e^{-2\pi i n x} |\varphi(x)\rangle \\ &= \sum_{\ell \in \mathbb{Z}} |\ell a\rangle \left(\int_0^{\frac{1}{a}} dx e^{-2\pi i \ell a x} |\varphi(x)\rangle \right) \\ &= \sum_{\ell \in \mathbb{Z}} |\ell a\rangle |\Omega(\ell a)\rangle \end{aligned}$$

• Step 4. Measure

$$|\psi_3\rangle = \sum_{\ell \in \mathbb{Z}} |\ell a\rangle |\Omega(\ell a)\rangle$$

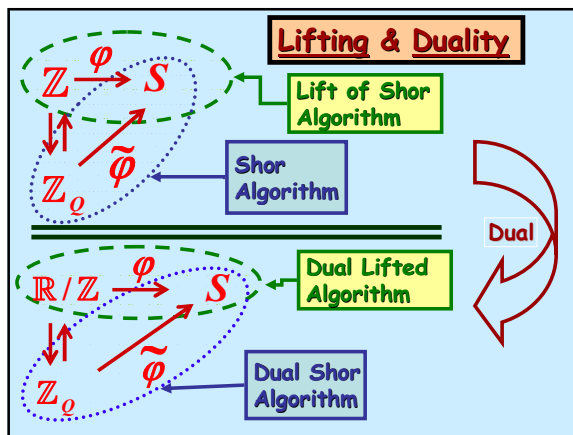
with respect to the observable

$$\mathcal{O} = \sum_{n \in \mathbb{Z}} n |n\rangle\langle n|$$

to produce a random eigenvalue ℓa

The
corresponding
discrete
algorithm

The Algorithmic Dual
of
Shor's Quantum
Factoring Algorithm



We now create a corresponding
discrete algorithm

The approximations are:

$$\mathbb{Z} \approx \mathbb{Z}_Q = \{k \in \mathbb{Z} : 0 \leq k < Q\}$$

$$\mathbb{R}/\mathbb{Z} \approx \mathbb{Z}_Q = \left\{ \frac{r}{Q} \bmod 1 : r = 0, 1, \dots, Q-1 \right\}$$

$$\varphi : \mathbb{Z} \rightarrow \mathbb{C} \approx \tilde{\varphi} : \mathbb{Z}_Q \rightarrow \mathbb{C}$$

$\tilde{\varphi}$ 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^2 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

$$\begin{cases} (\lambda x)(s) &= \lambda x(s) \\ (x+y)(s) &= x(s)+y(s) \end{cases}$$

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 **Paths** can be written as the following disjoint union:

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

- Step 0. Initialize

$$|\psi_0\rangle = |0\rangle|0\rangle \in \mathcal{H}_{\text{paths}} \otimes \mathcal{H}_{\mathbb{C}}$$

- Step 1. Apply $\mathcal{F}^{-1} \otimes 1$

$$|\psi_1\rangle = \int_{\text{Paths}} \mathcal{D}x e^{2\pi i x \cdot 0} |x\rangle|0\rangle = \int_{\text{Paths}} \mathcal{D}x |x\rangle|0\rangle$$

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

$$|\psi_2\rangle = \int_{\text{Paths}} \mathcal{D}x |x\rangle|\varphi(x)\rangle$$

- Step 3. Apply $\mathcal{F} \otimes 1$

$$\begin{aligned} |\psi_3\rangle &= \int_{\text{Paths}} \mathcal{D}y \int_{\text{Paths}} \mathcal{D}x e^{-2\pi i y \cdot y} |y\rangle|\varphi(x)\rangle \\ &= \int_{\text{Paths}} \mathcal{D}y |y\rangle \int_{\text{Paths}} \mathcal{D}x e^{-2\pi i y \cdot y} |\varphi(x)\rangle \end{aligned}$$

But

$$\int_{\text{Paths}} \mathcal{D}x e^{-2\pi i x \cdot y} |\varphi(x)\rangle = \int_V \mathcal{D}v \int_{V^\perp} \mathcal{D}x e^{-2\pi i x \cdot y} |\varphi(x)\rangle$$

$$= \int_V \mathcal{D}v \int_{V^\perp} \mathcal{D}x e^{-2\pi i (v+x) \cdot y} |\varphi(v+x)\rangle$$

$$= \int_V \mathcal{D}v e^{-2\pi i v \cdot y} \int_{V^\perp} \mathcal{D}x e^{-2\pi i x \cdot y} |\varphi(x)\rangle$$

However, $\int_V \mathcal{D}v e^{-2\pi i v \cdot y} = \int_{V^\perp} \mathcal{D}u \delta(y-u)$

So,

$$|\psi_3\rangle = \int_{\text{Paths}_n} \mathcal{D}y |y\rangle \int_V \mathcal{D}v e^{-2\pi i v \cdot y} \int_{V^\perp} \mathcal{D}x e^{-2\pi i x \cdot y} |\varphi(x)\rangle$$

$$= \int_{\text{Paths}_n} \mathcal{D}y |y\rangle \int_{V^\perp} \mathcal{D}u \delta(y-u) \int_{V^\perp} \mathcal{D}x e^{-2\pi i x \cdot y} |\varphi(x)\rangle$$

$$= \int_{V^\perp} \mathcal{D}u |u\rangle \int_{V^\perp} \mathcal{D}x e^{-2\pi i x \cdot u} |\varphi(x)\rangle$$

$$= \int_{V^\perp} \mathcal{D}u |u\rangle |\Omega(u)\rangle$$

•Step 4. Measure

$$|\psi_3\rangle = \int_{V^\perp} \mathcal{D}u |u\rangle |\Omega(u)\rangle$$

with respect to the observable

$$A = \int_{\text{Paths}} \mathcal{D}w w |w\rangle \langle w|$$

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?

$$\hat{\psi}(K) = \int \mathcal{D}A \psi(A) \mathcal{W}_K(A)$$

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

$$\mathcal{W}_K(A) = \text{tr} \left(P \exp \left(\oint_K A \right) \right)$$



Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium, Samuel J. Lomonaco, Jr. (editor), AMS PSAPM/58, (2002).



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

