Quantum Walks and Applications to Quantum Money

Seyed Ali Mousavi

Supervised by Dr. Jake Doliskani

March 26, 2025

Program and Courses Taken

- Program: M.A.Sc in Software Engineering

- CAS 701, Logic & Discrete Mathematics
- COMPSCI 6TE3, Continuous optimization
- CAS 721, Combinatorics & Computing
- CAS 741, Development of Scientific Computation Software

Seminars

- I have participated in 6 seminars during my program.

Poster

Quantum Walks For Quantum Money

Jake Doliskani, Ali Mousavi
Department of Computing and Software, McMaster University

McMaster University

Quantum Mechanic Postulates

- **State Postulate**: A qubit's state can be written as
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$
- **Measurement Postulate**: Measuring in the basis $\{|0\rangle, |1\rangle\}$ yields $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.
- **Evolution Postulate**: The qubit state $|\psi(t)\rangle$ evolves according to:
$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle,$$

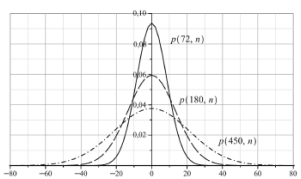
Quantum Walks

General equation:

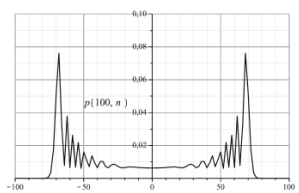
$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

Quantum walks serve as the foundation for various quantum algorithms, providing speedups in tasks like search and graph traversal, where they outperform classical approaches.

integer axis can indeed be considered as an infinite graph



Probability distribution of a classical Random walk on integer axis

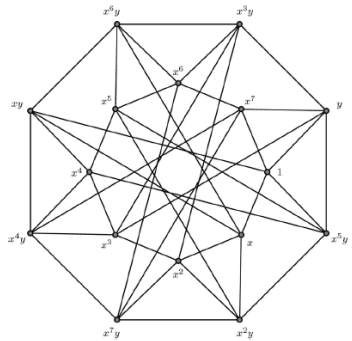


Probability distribution of a Qunatum walk on integer axis

Quantum Walk On Group Actions

- **Definition**: A group action of a group G on a set X is a way to combine each element g from G with elements x from X using an operation $*$ such that $g * x$ gives an element in X.
- **Properties**: The group action satisfies:
  Identity: The identity element e in G satisfies $e * x = x$ for all $x \in X$.
  Compatibility: For any $g, h \in G$ and $x \in X$, $(g \cdot h) * x = g * (h * x)$,
- **Importance in Cryptography**: Group actions create hard-to-reverse problems, forming the foundation for secure cryptographic protocols.

A Cayley graph is a specific example of a graph with a group action:



A sample Cayley graph

Why using Caley graphs for quantum walks?

- **Defines Movement Rules:** Cayley graphs set the structure and movement rules for quantum walks, using group elements to dictate transitions between vertices.
- **Enables Algorithm Design:** Their algebraic properties make them ideal for designing efficient quantum algorithms, like search and mixing-based algorithms.
- **Simplifies Analysis:** The group-theoretic structure aids in mathematical analysis, allowing for insights into walk behavior and performance in quantum applications.

Application: Quantum Money Verification

Quantum money is a combination of a classical value $|h\rangle$ and a quantum state $|\$\rangle$. The quantum money state is an eigenvector of the quantum walk operator. Using phase estimation, we extract the eigenvalue, which contains the money's serial number. This allows verification by checking if the extracted serial number matches the one on the money.

$$A = \sum_{k\in\mathbb{Z}_N} \lambda_k |k\rangle_F\langle k|_F$$

Where:

$$|k\rangle_F = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} \omega_N^{ky}|y\rangle, \omega_N = e^{\frac{2\pi i}{N}}$$

is the *quantum fourier transform(QFT)*. So:

$$e^{iAt} = \sum_{k\in\mathbb{Z}_N} e^{i\lambda_k t}|k\rangle_F\langle k|_F$$

Now if we apply the continous quantum walk e^{iAt} on the *Hartly transform* $|x\rangle_H$:

$$e^{iAt}|x\rangle_H = (\sum_{k\in\mathbb{Z}_N} e^{i\lambda_k t}|k\rangle_F\langle k|_F)(\frac{1-i}{2}|x\rangle_F + \frac{1+i}{2}|-x\rangle_F)$$
$$= \frac{1-i}{2}e^{i\lambda_x t}|x\rangle_F + \frac{1+i}{2}e^{i\lambda_{-x} t}|x\rangle_F = e^{i\lambda_x t}|x\rangle_H$$

Thus, the quantum money state is the eigenvector of our quantum walk operator. Therefore, For obtaining the value h (serial number) we can perform a *phase estimation* on the quantum walk operator e^{iAt}.

References

1 Zhandry, M., 2023. Quantum money from abelian group actions. arXiv preprint arXiv:2307.12120.
2 Childs, A. M. (2009). On the relationship between continuous- and discrete-time quantum walks. arXiv preprint arXiv:0810.0312.
3 Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A. and Shor, P., 2012, January. Quantum money from knots. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (pp. 276-289).

Figure: Presented at Nov. 6, 2024

Quantum Computation - Preliminaries and Notation

- Consider a finite Hilbert space $\mathcal{H}$ with an orthonormal set of basis states $\{|s_i\rangle\}$ for $s \in \mathcal{S}$. The states $s \in \mathcal{S}$ may be interpreted as the possible classical states of the system described by $\mathcal{H}$.

- In general, the state of the system, $|\alpha\rangle$, is a unit vector in the Hilbert space $\mathcal{H}$ and can be written as $|\alpha\rangle = \sum_{s\in\mathcal{S}} a_s|s\rangle$, where $\sum_{s\in\mathcal{S}} |a_s|^2 = 1$.

- $\langle\alpha|$ denotes the conjugate transpose of $|\alpha\rangle$. The expression $\langle\beta|\alpha\rangle$ denotes the inner product of $|\alpha\rangle$ and $|\beta\rangle$.

Quantum Computation - Quantum Postulates

- **Unitary evolution**: Quantum physics requires that the evolution of quantum states is unitary; that is, the state $|\alpha\rangle$ is mapped to $U|\alpha\rangle$, where U satisfies $U \cdot U^{\dagger} = I$, and $U^{\dagger}$ denotes the conjugate transpose of U.

- **Measurement**: We will describe here only a measurement in the orthonormal basis $|s\rangle$. The output of the measurement of the state $|\alpha\rangle$ is an element $s \in \mathcal{S}$, with probability $|\langle s|\alpha\rangle|^2$. Moreover, the new state of the system after the measurement is $|s$.

- **Combining two quantum systems**: If $\mathcal{H}_A$ and $\mathcal{H}_B$ are the Hilbert spaces of two systems, A and B, then the joint system is described by the tensor product of the Hilbert spaces, $\mathcal{H}_A \otimes \mathcal{H}_B$. If the basis states for $\mathcal{H}_A$ and $\mathcal{H}_B$ are $\{|a_i\rangle\}$ and $\{|v_i\rangle\}$ respectively, then the basis states of $\mathcal{H}_A \otimes \mathcal{H}_B$ are $\{|a_i\rangle \otimes |v_i\rangle\}$.

The Hartley Transform

item Let N be a positive integer, and let $\mathbb{Z}_N$ be the additive cyclic group of integers modulo N. The Hartley transform of a function $f : \mathbb{Z}_N \to \mathbb{R}$ is the function $\mathrm{H}_N(f) : \mathbb{Z}_N \to \mathbb{R}$ defined by

$$\mathrm{H}_N(f)(a) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \mathrm{cas}\left(\frac{2\pi a y}{N}\right) f(y),$$

where $\mathrm{cas}(x) = \cos(x) + \sin(x)$
For a single basis element of the cyclic group $\mathbb{Z}_N$, the quantum Hartly transform simplifies to

$$\mathrm{QHT}_N : |a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \mathrm{cas}\left(\frac{2\pi a y}{N}\right) |y\rangle \,. \tag{1}$$

An efficient new algorithm for QHT

First, let us briefly explain how the algorithm for QFT_N works:

$$\begin{aligned}
\mathrm{QFT}_N |a\rangle &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{ay} |y\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{y=0}^{N/2-1} \omega_N^{ay} |y\rangle + (-1)^a \sum_{y=0}^{N/2-1} \omega_N^{ay} |y + N/2\rangle \\
&= \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \omega_N^{ay} \frac{1}{\sqrt{2}} (|0\rangle + (-1)^a |1\rangle) |y\rangle , \qquad (2)
\end{aligned}$$

An efficient new algorithm for QHT

Let $|a\rangle = |t\rangle\,|b\rangle$, where b is the least significant bit of a, so that $a = 2t + b$. Applying $\mathrm{QFT}_{N/2}$ to the first register, we obtain the state

$$\frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \omega_N^{2ty}\,|y\rangle\,|b\rangle\,.$$

Next, we apply the phase unitary $P(y,b) : |y\rangle\,|b\rangle \mapsto \omega_N^{by}\,|y\rangle\,|b\rangle$, and finally, we apply a Hadamard transform to the last qubit. The result is the state in (2).

An efficient new algorithm for QHT

$$\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \operatorname{cas}\left(\frac{2\pi a y}{N}\right) |y\rangle \tag{3}$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{2\pi a y}{N}\right) |y\rangle + \frac{1}{\sqrt{N}} \sum_{y=N/2}^{N-1} \operatorname{cas}\left(\frac{2\pi a y}{N}\right) |y\rangle \,. \tag{4}$$

The second sum in the right-hand side can be written as

$$\sum_{y=N/2}^{N-1} \operatorname{cas}\left(\frac{2\pi a y}{N}\right) |y\rangle = \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{2\pi a y}{N} + \pi a\right) |y + N/2\rangle$$

$$= (-1)^a \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{2\pi a y}{N}\right) |y + N/2\rangle \,,$$

An efficient new algorithm for QHT

$$= \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{2\pi a y}{N}\right) \frac{1}{\sqrt{2}} (|0\rangle + (-1)^a |1\rangle) |y\rangle , \tag{5}$$

We now show how to compute QHT_N recursively.

$$|0\rangle |t\rangle |b\rangle \mapsto \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{2\pi t y}{N/2}\right) |0\rangle |y\rangle |b\rangle$$

$$= \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{4\pi t y}{N}\right) |0\rangle |y\rangle |b\rangle$$

$$\mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{4\pi t y}{N}\right) (|0\rangle + |1\rangle) |y\rangle |b\rangle .$$

An efficient new algorithm for QHT

Algorithm (QHT_N)

- Input: quantum state $|\psi\rangle \in \mathbb{C}^N$, where $N = 2^n$
- Output: quantum state $\mathrm{QHT}_N |\psi\rangle$

1- Initialize an ancilla qubit to 0 to obtain the state $|0\rangle |\psi\rangle$
2- Compute $1 \otimes \mathrm{QHT}_{N/2} \otimes 1$ recursively.
3- Apply $H \otimes 1$.
4- Apply the controlled negation $|0\rangle |y\rangle \mapsto |0\rangle |y\rangle, |1\rangle |y\rangle \mapsto |1\rangle |N/2 - y\rangle$ to the first two registers.
5- Apply the unitary U_R.
6- Apply $H \otimes 1$
7- Apply CNOT to the first and last qubits.
8- Apply $1 \otimes H$.
9- Trace out the first qubit

Application: Quantum Money

A public-key quantum money scheme consists of two QPT algorithms:

- $\mathrm{Gen}(1^\lambda)$: This algorithm takes a security parameter λ as input and outputs a pair (s, ρ_s), where s is a binary string called the serial number, and ρ_s is a quantum state called the banknote. The pair (s, ρ_s), or simply ρ_s, is sometimes denoted by \$.

- $\mathrm{Ver}(s, \rho_s)$: This algorithm takes a serial number and an alleged banknote as input and outputs either 1 (accept) or 0 (reject).

Quantum Money From Group Actions

- $\mathrm{Gen}(1^\lambda)$. Begin with the state $|0\rangle |x_\lambda\rangle$, and apply the quantum Fourier transform over G_λ to the first register producing the superposition

$$\frac{1}{\sqrt{|X_\lambda|}} \sum_{g \in G_\lambda} |g\rangle |x_\lambda\rangle .$$

Next, apply the unitary transformation $|h\rangle |y\rangle \mapsto |h\rangle |h * y\rangle$ to this state, followed by the quantum Fourier transform on the first register. This results in

$$\frac{1}{|G_\lambda|} \sum_{h \in G_\lambda} \sum_{g \in G_\lambda} \chi(g,h) |h\rangle |g * x_\lambda\rangle = \frac{1}{\sqrt{|G_\lambda|}} \sum_{h \in G_\lambda} |h\rangle |G^{(h)} * x_\lambda\rangle$$

Quantum Money From Group Actions

- $\mathsf{Ver}(h, |\psi\rangle)$. First, check whether $|\psi\rangle$ has support in X_λ. If not, return 0. Then, apply cmpIndex to the state $|\psi\rangle|0\rangle$, and measure the second register to obtain some $h' \in G_\lambda$. If $h' = h$, return 1; otherwise return 0.

Quantum Money With The Hartley Transform

- Gen. Begin with the state $|0\rangle |x\rangle$, and apply the quantum Hartley transform over $\mathbb{Z}_N$ to the first register producing the superposition

$$\frac{1}{\sqrt{N}} \sum_{g \in \mathbb{Z}_N} |g\rangle |x\rangle .$$

Next, apply the unitary $|h\rangle |y\rangle \mapsto |h\rangle |h * y\rangle$ to this state, followed by a QHT_N on the first register. This results in

$$\frac{1}{N} \sum_{h \in \mathbb{Z}_N} \sum_{g \in \mathbb{Z}_N} \mathrm{cas}\left(\frac{2\pi gh}{N}\right) |h\rangle |g * x\rangle = \frac{1}{\sqrt{N}} \sum_{h \in \mathbb{Z}_N} |h\rangle |\mathbb{Z}_N^{(h)} * x\rangle_H$$

Measure the first register to obtain a random $h \in \mathbb{Z}_N$, collapsing the state to $|\mathbb{Z}_N^{(h)} * x\rangle_H$. Return the pair $(h, |\mathbb{Z}_N^{(h)} * x\rangle_H)$.

Quantum Money With The Hartley Transform

- In the original scheme, using the quantum Fourier transform, we could directly obtain h from the money state $|\mathbb{Z}_N^{(h)} * x\rangle$ and compare it to the given h. However, this approach does not work when we use the Hartley transform.

- To address this, we design an algorithm for computing h that utilizes quantum walks.

Quantum Walks

- Quantum walks are quantum analogs of classical random walks and play a fundamental role in quantum algorithms
- Two types: continuous-time and discrete-time
- Quantum walks leverage interference to explore graphs more efficiently than classical walks
- For a graph Γ, a continuous-time classical walk on Γ is:

$$\frac{d}{dt}q(t) = Lq(t)$$

- In the quantum setting, the dynamics of the walk is given by the Schrödinger equation:

$$i\frac{d}{dt}\left|\psi(t)\right\rangle = L\left|\psi(t)\right\rangle$$

Continuous-Time Quantum Walks

- The solution to this differential equation can be written in closed form as:

$$|\psi(t)\rangle = e^{-iLt} |\psi(0)\rangle .$$

- In practice, we often (including this work) use the adjacency matrix A of Γ as the Hamiltonian of the walk

Discrete-Time Quantum Walks

- If the Γ has N vertices, the discrete time quantum walk on Γ is defined by a unitary operator on the finite Hilbert space $\mathbb{C}^N \times \mathbb{C}^N$ as follows:
- Define the states:

$$|\phi_j\rangle = \frac{1}{\sqrt{\deg(j)}} \sum_{k=1}^{N} |j,k\rangle ,$$

- project and swap operators:

$$\Pi = \sum_{j=1}^{N} |\phi_j\rangle \langle \phi_j| , \quad S = \sum_{j,k=1}^{N} |j,k\rangle \langle k,j| .$$

- Then, a step of the quantum walk is defined by the unitary:

$$W = S(2\Pi - 1)$$

Quantum Walks on Cayley Graphs

Cayley Graphs:

Let G be an abelian group and let $Q = \{q_1, q_2, \ldots, q_k\} \subset G$ be a symmetric set, i.e., $q \in Q$ if and only if $-q \in Q$. The Cayley graph associated to G and Q is a graph $\Gamma = (V, E)$, where the vertex set is $V = G$, and the edge set E consists of pairs $(a, b) \in G \times G$ such that there exists $q \in Q$ with $b = q + a$.

Quantum Walks on Cayley Graphs

Cayley Graphs:

The adjacency matrix of the Cayley graph $\Gamma = (V, E)$ can be expressed as:

$$A = \sum_{a \in G} \lambda_a \left|\hat{a}\right\rangle \left\langle\hat{a}\right|,$$

where $\left|\hat{a}\right\rangle = \mathrm{QFT}\left|a\right\rangle$ is the quantum Fourier transform of $\left|a\right\rangle$.

The eigenvalues λ_a are given by:

$$\lambda_a = \sum_{q \in Q} \chi(a, q).$$

Note that the eigenvectors $\left|\hat{a}\right\rangle$ of A depend only on G and not on the set Q.

Quantum Walks on Cayley Graphs

Cayley Graphs:

proofs:

Group Actions

Cayley graphs can also be constructed using *group actions*.

Group Actions:

For a group G and a set X, we say that G *acts on* X if there is a mapping $* : G \times X \to X$ that satisfies the following properties:

1. Compatibility: for every $a, b \in G$ and every $x \in X$, $g * (h * x) = (gh) * x$,
2. Identity: for the identity $1 \in G$ and every $x \in X$, $1 * x = x$.

- We use the notation $(G, X, *)$ to denote a group G acting on a set X through the action $*$.
- A group action is called *regular* if for every $x, y \in X$ there exists a unique $g \in G$ such that $g * x = y$.

Cayley Graphs with Group Actions

Given a regular group action $(G, X, *)$ with a fixed element $x \in X$ and a set $Q = \{q_1, q_2, \ldots, q_k\} \subset G$, let $\Gamma = (X, E)$ be a graphs with vertex set X and edge set consisting of pairs $(x, y) \in X \times X$ such that $y = q * x$ for some $q \in Q$. The adjacency matrix of Γ is

$$A = \sum_{h \in G} \lambda_h \left| G^{(h)} * x \right\rangle \left\langle G^{(h)} * x \right|,$$

where $\lambda_h = \sum_{q \in Q} \chi(h, q)$. Again, the eigenvectors $\left| G^{(h)} * x \right\rangle$ depend only on G.

Cayley Graphs with Group Actions

proofs:

Group Action Quantum Walks

Given a regular group action $(G, X, *)$ with a fixed element $x \in X$ and a set $Q = \{q_1, q_2, \ldots, q_k\} \subset G$, let $\Gamma = (X, E)$ be a graphs with vertex set X and edge set consisting of pairs $(x, y) \in X \times X$ such that $y = q * x$ for some $q \in Q$. The adjacency matrix of Γ is

$$A = \sum_{h \in G} \lambda_h \left| G^{(h)} * x \right\rangle \left\langle G^{(h)} * x \right|,$$

where:

- $\lambda_h = \sum_{q \in Q} \chi(h, q)$
- the eigenvectors $\left| G^{(h)} * x \right\rangle$ depend only on G

Computing the serial Number

- Given a state $|\mathbb{Z}_N^{(h)} * x\rangle_H$, we show how to compute h using continuous-time quantum walks.
- For any $q \in \mathbb{Z}_N$, define a Cayley graph $\Gamma = (\mathbb{Z}_N, E)$ with the generating set $Q = \{-u, u\}$.
- Let A denote the adjacency matrix of Γ. The eigenvectors and corresponding eigenvalues of A are $|\mathbb{Z}_N^{(h)} * x\rangle$ and $\lambda_h = 2\cos(2\pi uh/N)$, respectively, for $h \in \mathbb{Z}_N$.
- the unitary $W = e^{iAt}$ can be efficiently simulated to exponential accuracy.

Computing the serial Number

Lemma: The money state $|\mathbb{Z}_N^{(h)} * x\rangle_H$ is an eigenstate of W with eigenvalue $e^{i\lambda_h t}$.

Proof.

$$
\begin{aligned}
e^{iAt} |\mathbb{Z}_N^{(h)} * x\rangle_H &= \sum_{g \in \mathbb{Z}_N} e^{i\lambda_g t} |\mathbb{Z}_N^{(g)} * x\rangle \langle \mathbb{Z}_N^{(g)} * x | \mathbb{Z}_N^{(h)} * x\rangle_H \\
&= \sum_{g \in \mathbb{Z}_N} e^{i\lambda_g t} |\mathbb{Z}_N^{(g)} * x\rangle \langle \mathbb{Z}_N^{(g)} * x | \left(\frac{1-i}{2} |\mathbb{Z}_N^{(h)} * x\rangle + \frac{1+i}{2} |\mathbb{Z}_N^{(} \right. \\
&= e^{i\lambda_h t} \frac{1-i}{2} |\mathbb{Z}_N^{(h)} * x\rangle + \frac{1+i}{2} e^{i\lambda_{-h} t} |\mathbb{Z}_N^{(-h)} * x\rangle \\
&= e^{i\lambda_h t} |\mathbb{Z}_N^{(h)} * x\rangle_H ,
\end{aligned}
$$

where the last equality follows from the fact that $\lambda_h = \lambda_{-h}$.

Computing the serial Number

Lemma: The money state $|\mathbb{Z}_N^{(h)} * x\rangle_H$ is an eigenstate of W with eigenvalue $e^{i\lambda_h t}$.

$$e^{iAt} |\mathbb{Z}_N^{(h)} * x\rangle_H = e^{i\lambda_h t} |\mathbb{Z}_N^{(h)} * x\rangle_H$$

If we choose $t = \text{poly}(\log N)$, it follows from Lemma that we can run the phase estimation algorithm with the unitary W and the eigenstate $|\mathbb{Z}_N^{(h)} * x\rangle_H$ to compute an estimate $\tilde{\lambda}_h$ of λ_h such that

$$|\tilde{\lambda}_h - \lambda_h| \leq \frac{1}{\text{poly}(\log N)}$$