Quantum Notation and Quantum Computing

Seyed Ali Mousavi

March 2, 2025

Courses Taken

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

Seminars

-

Application: Quantum Money

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

- Gen(1^λ): 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 \$.
- 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

- $\mathsf{Gen}(1^\lambda)$. 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
$$\frac{1}{|G_\lambda|}\sum_{h\in G_\lambda}\sum_{g\in G_\lambda}\chi(g,h)\,|h\rangle\,|g * x_\lambda\rangle = \frac{1}{\sqrt{|G_\lambda|}}\sum_{h\in G_\lambda}|h\rangle\,|G^{(h)} * x_\lambda\rangle$$
where $|G^{(h)} * x_\lambda\rangle$ is defined as in (**??**). Measure the first register to obtain a random $h \in G_\lambda$, collapsing the state to $|G^{(h)} * x_\lambda\rangle$. Return the pair $(h, |G^{(h)} * x_\lambda\rangle)$.
- $\mathsf{Ver}(h, |\psi\rangle)$. First, check whether $|\psi\rangle$ has support in X_λ. If not,

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

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

where

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

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 $(h, |\mathbb{Z}_N^{(h)} * x\rangle_H)$.

Group Action Quantum Walks

Let G be an abelian group and let $Q = \{q_1, q_2, \dots, q_k\} \subset G$ 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 $b = q + a$. The adjacency matrix of Γ can be expressed as

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

where $|\hat{a}\rangle$ is the quantum Fourier transform of $|a\rangle$. The eigenvalues λ are given by

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

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

Group Action Quantum Walks

Cayley graphs can also be constructed using 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 $|G^{(h)} * x\rangle$ depend only on G. This construction of Cayley graphs from group actions generalizes the previous construction. Specifically, if we set $X = G$ and the action $*$ as group operation, we recover the original construction.
Since the action $(G, X, *)$ is regular, the two constructions yield the same graph up to isomorphism. In the first graph, the vertex set is G, and the rows and columns of the adjacency matrix are indexed by the elements of G, whereas in the second graph, the vertex set is X, and the rows and columns of the adjacency matrix are indexed by the elements of X. The

Introduction to Quantum Notation

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

We have :

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

where the second equality follows from the identity in (**??**), and the last equality follows from the fact that $\lambda_h = \lambda_{-h}$.