Quantum Notation and Quantum Computing

Seyed Ali Mousavi

March 3, 2025

Courses Taken

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

Seminars

-

Poster

-

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

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

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

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

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

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

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

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

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

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.

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

An efficient new algorithm for QHT

$$= \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \operatorname{cas}\left(\frac{2\pi ay}{N}\right) \frac{1}{\sqrt{2}} (|0\rangle + (-1)^a |1\rangle) |y\rangle , \tag{6}$$

We now show how to compute QHT_N recursively.

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

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

- Gen(1^λ). 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

- 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

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

  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.

Group Action Quantum Walks

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 $b = q + a$. 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 $\left|\hat{a}\right\rangle$ is the quantum Fourier transform of $\left|a\right\rangle$. The eigenvalues λ 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.

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:

- $\lambda_h = \sum_{q \in Q} \chi(h, q)$
- 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 $Q = \{-q, q\}$. 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. We need the following lemma.

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.

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

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