Quantum Walks and Applications to Quantum Money

Seyed Ali Mousavi

Supervised by Dr. Jake Doliskani

March 29, 2025

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 $\{|a_i\rangle \otimes |v_i\rangle\}$.

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

Example of a Continuous Quantum 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:

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

▶ 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:

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

Example of a Discrete-Time Quantum Walk

Continuous vs Discrete Quantum Walks

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 $b = q + a$.

An Example of a Cayley Graph

Quantum Walks on Cayley Graphs

Cayley Graphs:

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

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

where $|\hat{a}\rangle = \text{QFT}_G \, |a\rangle$ is the *Quantum Fourier transform (QFT)* of $|a\rangle$.

... But, What is QFT??

Quantum Fourier Transform (QFT)

Let G be an abelian group. The set of characters of G, denoted by $\hat{G}$, is the set of homomorphisms $\chi(a, \cdot) : G \to \mathbb{C}$ where $a \in G$. If $G \cong \mathbb{Z}_{N_1} \oplus \cdots \oplus \mathbb{Z}_{N_k}$ then the character $\chi(a, \cdot)$ can be explicitly written as

$$\chi(a, x) = \omega_{N_1}^{a_1 x_1} \cdots \omega_{N_k}^{a_k x_k}$$

where $\omega_M = \exp(2\pi i / M)$ is a primitive M-th root of unity. The Fourier transform of a function $f : G \to \mathbb{C}$ is given by

$$\hat{f}(a) = \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi(a, x) f(x).$$

The quantum Fourier transform:

$$\sum_{g \in G} f(g) \left| g \right\rangle \mapsto \sum_{x \in G} \hat{f}(x) \left| x \right\rangle$$

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 $\left| \hat{a} \right\rangle = \mathrm{QFT}_G(\left| a \right\rangle) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi(a, g) \left| g \right\rangle$.

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:

Proof:

$$A \ket{\hat{a}} = A. \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi(a,y) \ket{y} = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi(a,y).A \ket{y}$$

$$= \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi(a,y). \sum_{q \in Q} \ket{qy}$$

Consider $\beta = qy$. Then:

$$= \frac{1}{\sqrt{|G|}} \sum_{q \in Q} \chi(a,q) \sum_{\beta} \chi(a,\beta) \ket{\beta} = \sum_{q \in Q} \chi(a,q). \ket{\hat{a}}$$

$$= \lambda_a \ket{\hat{a}}$$

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:

$$\left| G^{(h)} * x \right\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi(g, h) \left| g * x \right\rangle$$

And $\lambda_h = \sum_{q \in Q} \chi(h, q)$.

▶ Again, the eigenvectors $\left| G^{(h)} * x \right\rangle$ depend only on G.

Cayley Graphs with Group Actions

Proof:

$$A \left| G^{(h)} * x \right\rangle = \frac{1}{\sqrt{|G|}} \cdot \sum_{g \in G} \chi(g, h) A. \left| g * x \right\rangle$$

$$= A \left| G^{(h)} * x \right\rangle = \frac{1}{\sqrt{|G|}} \cdot \sum_{g \in G} \chi(g, h) \sum_{q \in Q} \left| q * (g * x) \right\rangle$$

Consider $\beta = qg$. Then:

$$== \frac{1}{\sqrt{|G|}} \sum_{q \in Q} \sum_{\beta \in G} \chi(\beta, h) \chi(q, h) \left| \beta * x \right\rangle$$

$$= \sum_{q \in Q} \chi(q, h). \left| G^{(h)} * x \right\rangle = \lambda_h \left| G^{(h)} * x \right\rangle$$

The cmpIndex Algorithm

Given a state $|G^{(h)} * x\rangle$, there is an efficient algorithm for computing h. Specifically, there is a unitary operator that performs the transformation $|G^{(h)} * x\rangle |0\rangle \mapsto |G^{(h)} * x\rangle |h\rangle$:

$$|G^{(h)} * x\rangle |0\rangle \mapsto |G^{(h)} * x\rangle \frac{1}{\sqrt{|G|}} \sum_{k \in G} |k\rangle$$

And then apply the unitary $\sum_{k \in G} U_k \otimes |k\rangle \langle k|$:

$$\mapsto \frac{1}{\sqrt{|G|}} \sum_{k \in G} |G^{(h)} * x\rangle \chi(-k, h) |k\rangle$$

Finally, applying the inverse quantum Fourier transform to the second register yields:

$$\mapsto |G^{(h)} * x\rangle |h\rangle$$

Simulating continuous-time walks

$$|\phi_{j0}\rangle := \frac{1}{\sqrt{d}} \sum_{l \in F_j} (\sqrt{\frac{H_{jl}^*}{K}} |0\rangle + \sqrt{1 - \frac{|H_{jl}^*|}{K}} |1\rangle)$$

$$|\phi_{j1}\rangle := |0\rangle |1\rangle$$

$$T := \sum_{j=0}^{N-1} \sum_{b \in \{0,1\}} (|j\rangle\langle j| \otimes |b\rangle\langle b|) \otimes |\phi_{jb}\rangle$$

$$W = iS(2TT^* - 1)$$

$$S|j_1, b_1\rangle |j_2, b_2\rangle = |j_2, b_2\rangle |j_1, b_1\rangle$$

Simulating continuous-time walks

$$e^{-iAt} = \mathsf{QFT}_\mathsf{G}\Big(\sum_{a \in G} e^{-i\lambda_a t} \ket{a}\bra{a}\Big)\mathsf{QFT}_\mathsf{G}^*$$

Simulating group action quantum walks

$$2\ket{0}\bra{0} \otimes TT^* - 1 = 2\ket{0}\bra{0} \otimes \sum_{y \in X} \sum_{b \in \{0,1\}} \ket{y,b}\ket{\phi_{yb}}\bra{y,b}\bra{\phi_{yb}} - 1$$

$$= 2 \sum_{y \in X} \sum_{b \in \{0,1\}} \ket{0}\ket{y,b}\ket{\phi_{yb}}\bra{0}\bra{y,b}\bra{\phi_{yb}} - 1$$

$$= U_T\Big(2 \sum_{y \in X} \sum_{b \in \{0,1\}} \ket{0}\ket{y,b}\ket{0,0}\bra{0}\bra{y,b}\bra{0,0} - 1\Big)U_T^*$$

$$= U_T(2\ket{0}\bra{0} \otimes 1_{X,b} \otimes \ket{0,0}\bra{0,0} - 1)U_T^*$$

Now, for any state $\ket{\psi}$:

$$(2\ket{0}\bra{0} \otimes TT^* - 1)\ket{0}\ket{\psi} = \ket{0}(2TT^* - 1)\ket{\psi}$$

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

Application: Quantum Money

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

- ▶ $\text{Gen}(1^\lambda)$: 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 \$.

- ▶ $\text{Ver}(s, \rho_s)$: 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

▶ $\text{Gen}(1^\lambda)$. 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

▶ $\text{Ver}(h, |\psi\rangle)$. 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

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 $H_N(f) : \mathbb{Z}_N \to \mathbb{R}$ defined by

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

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

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

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

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

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.

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:

$$e^{iAt} |\mathbb{Z}_N^{(h)} * x\rangle_H = \sum_{g \in \mathbb{Z}_N} e^{i\lambda_g t} |\mathbb{Z}_N^{(g)} * x\rangle \langle \mathbb{Z}_N^{(g)} * x | \mathbb{Z}_N^{(h)} * x\rangle_H$$

$$= \sum_{g \in \mathbb{Z}_N} e^{i\lambda_g t} |\mathbb{Z}_N^{(g)} * x\rangle \langle \mathbb{Z}_N^{(g)} * x | \left(\frac{1-i}{2} |\mathbb{Z}_N^{(h)} * x\rangle + \frac{1+i}{2} |\mathbb{Z}_N^{(-h)} * x\rangle \right)$$

$$= e^{i\lambda_h t} \frac{1-i}{2} |\mathbb{Z}_N^{(h)} * x\rangle + \frac{1+i}{2} e^{i\lambda_{-h} t} |\mathbb{Z}_N^{(-h)} * x\rangle$$

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

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

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

An efficient new algorithm for QHT

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

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

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

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

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

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

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

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

An efficient new algorithm for QHT

$$= \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \mathrm{cas}\Big(\frac{2\pi ay}{N}\Big) \frac{1}{\sqrt{2}} (|0\rangle + (-1)^a |1\rangle) |y\rangle, \qquad (5)$$

We now show how to compute QHT_N recursively.

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

$$= \frac{1}{\sqrt{N/2}} \sum_{y=0}^{N/2-1} \mathrm{cas}\Big(\frac{4\pi ty}{N}\Big) |0\rangle |y\rangle |b\rangle$$

$$\mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N/2-1} \mathrm{cas}\Big(\frac{4\pi ty}{N}\Big) (|0\rangle + |1\rangle) |y\rangle |b\rangle.$$

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 $QHT_N |\psi\rangle$

1- Initialize an ancilla qubit to 0 to obtain the state $|0\rangle |\psi\rangle$

2- Compute $1 \otimes QHT_{N/2} \otimes 1$ 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

References