Kyung Hee University
Communications and Quantum Information Laboratory

Notes : Introduction to Quantum Algorithms

Amirul Adlil Hakim
Director: Hyundong Shin

(This is a note that I made by myself to study quantum algorithms from [1]. All the contents was in the original source, I just paraphrased it here.)

1 Preliminaries on quantum computation

1.1 Postulates on quantum mechanics

1.1.1 State space postulate

A state space is a complex vector space with inner product structure, known as the Hilbert space $\mathcal{H}$, that is formed by a set of all quantum states of a quantum system. The space $\mathcal{H}$ is isomorphic to some $\mathbb{C}^N$ if it is finite dimensional, and can be taken as $\mathcal{H} = \mathbb{C}^N$. We assume that $N = 2^n$ for some non-negative integer n which we will refer as qubits. A quantum state $\psi \in \mathbb{C}^N$ can be expressed in terms of its components as

$$\psi = \begin{bmatrix} \psi_0 \\ \psi_1 \\ \cdot \\ \cdot \\ \psi_{N-1} \end{bmatrix}, \tag{1}$$

that has a Hermitian conjugate which is

$$\psi^\dagger = \begin{bmatrix} \psi_0^* & \psi_1^* & \cdot & \cdot & \psi_{N-1}^* \end{bmatrix}. \tag{2}$$

We use the Dirac notation, $|\psi\rangle$ for the quantum state and $\langle \psi^\dagger|$ for its Hermitian conjugate. Using this notation, we can denote the inner product between two quantum states as below

$$\langle \psi | \phi \rangle = \psi^\dagger \phi = \sum_{i=0}^{N-1} \psi_i^* \phi_i. \tag{3}$$

We can denote the basis of $\mathbb{C}^N$ as $\{|i\rangle\}$, then to find the i-th component of $|\phi\rangle$, we can use the inner product $|\phi_i\rangle = \langle i|\phi\rangle$. A projection operator can be defined as a matrix that is constructed by the outer product $\langle \phi| |\psi\rangle$. To find the (i, j)-th component of the projection operator matrix, we can use

$$\langle i| |\phi\rangle \langle \psi| |j\rangle = \langle i|\phi\rangle \langle \psi|j\rangle. \tag{4}$$

We assume that the state $|\psi\rangle$ is always normalized, $\langle \psi|\psi\rangle = 1$, because the state vectors $|\psi\rangle$ and $c|\psi\rangle$ correspond to the same physical state. If $|\phi\rangle$ is normalized, then $c = e^{i\theta}$ for some $\theta \in [0, 2\pi)$, which we refer as the global phase.

For example, a single qubit can be expressed as a vector that lives in $\mathcal{H} = \mathbb{C}^2$. We can choose one basis for this Hilbert space, namely

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{5}$$

In the context of spin-$\frac{1}{2}$ system which the space state is isomorphic to $\mathbb{C}^2$, the basis above can be seen as representing the spin-up ($|0\rangle$) and spin-down ($|1\rangle$). By using this basis, we can represent a general vector in this space state

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha |0\rangle + \beta |1\rangle, \tag{6}$$

which implies $|\alpha|^2 + |\beta|^2 = 1$ because of normalization. More generally, we can write $|\psi\rangle$ as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \cos(\theta/2) |0\rangle + e^{i\phi} \sin(\theta/2) |1\rangle, \tag{7}$$

where $0 \leq \theta < \pi$, $0 \leq \psi < 2\pi$. By using these angles, we can represent any single qubit state in a three-dimensional sphere known as the Bloch Sphere, where each state can be represented As

$$a = (\sin\theta \cos\psi, \sin\theta \sin\psi, \cos\theta)^T. \tag{8}$$

1.1.2 Quantum operator postulate

A quantum state can evolve from $|\psi\rangle \rightarrow \left|\psi'\right\rangle \in \mathbb{C}^N$ if a unitary operator $U \in \mathbb{C}^{N\times N}$ acts on it, such that

$$\left|\psi'\right\rangle = U |\psi\rangle. \tag{9}$$

The gate in quantum computing typically use this unitary operator, one example is the Pauli matrices defined as follows

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{10}$$

Another examples are the Hadamard gate, the phase gate, and the T gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \tag{11}$$

As mentioned before,the evolution of a quantum state at time t_1 into t_2 is caused by a unitary operator $U(t_2, t_1)$, in which the two quantum states has a linear relation

$$|\psi(t_2)\rangle = U(t_2, t_1) |\psi(t_1)\rangle. \tag{12}$$

If a time-independent Hamiltonian acts on a quantum state, then we have the following Schrödinger equation,

$$i\frac{d |\psi(t)\rangle}{dt} = H |\psi(t)\rangle, \tag{13}$$

where $H = H^\dagger$ is Hermitian. From the above equation, we can obtain the time evolution operator based on the Hamiltonian

$$U(t_2, t_1) = e^{-iH(t_2 - t_1)}. \tag{14}$$

1.1.3 Quantum measurement postulate

The type of quantum measurement that will be discussed here is the projective measurement. The projective measurement can be used to express all quantum measurements of the type positive operator-valued measure (POVM).

Any finite dimensional quantum observable can be represented by a Hermitian matrix that has spectral decomposition

$$M = \sum_{m=0}^{M-1} \lambda_m P_m, \tag{15}$$

where $\lambda_m \in \mathbb{R}$ are the eigenvalues of M and P_m are the projection operator onto the eigenspace of λ_m. The measurement of a quantum state by an observable M will always result in one of its eigenvalues λ_m with probability

$$p(m) = \langle\psi| P_m |\psi\rangle . \tag{16}$$

A measurement will change the quantum state in a non-unitary manner

$$\left|\psi'\right\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{17}$$

To calculate the expectation value of a quantum observable, we first notice that

$$\sum_m P_m = I \implies \sum_m p_m = \sum_m \langle\psi| P_m |\psi\rangle = 1. \tag{18}$$

This and the fact that $p_m \geq 0$ implies that $\{p_m\}$ is a probability distribution. Therefore, the expectation value of the measurement outcome can be calculated as

$$\mathbb{E}_\psi(M) = \sum_m \lambda_m p(m) = \sum_m \lambda_m \langle\psi| P_m |\psi\rangle = \left\langle \psi \middle| \sum_m \lambda_m P_m \middle| \psi \right\rangle = \langle\psi| M |\psi\rangle . \tag{19}$$

As an example, suppose that $M = X$, then

$$X |\pm\rangle = \lambda_\pm |\pm\rangle , \tag{20}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $\lambda_\pm = \pm 1$. From this, we can obtain the eigendecomposition of M,

$$M = X = |+\rangle \langle+| - |-\rangle \langle-| . \tag{21}$$

If we have a quantum state $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$, then the expectation value of X is $\frac{1}{2}$.

2 Grover's algorithm

2.1 Deutsch's algorithm

The problem that this algorithm can solve can be analoized as this one: We have two boxes, each of them may contain either an apple or an orange. How do we know if the two boxes contain the same fruit or not? We can open the two boxes to know the type of the fruit in each box, it is impossible to know whether the two boxes contain the same fruits or not without knowing them. Deutsch's algorithm tries to solve this problem without knowing the fruit in each box. This kind of problem can be modelled mathematically as follows: Consider a boolean function $f : \{0, 1\} \to$

$\{0,1\}$, the question is whethere $f(0) = f(1)$ or $f(0) \neq f(1)$. A quantum fruit-checker uses a quantum oracle to implement a function f such as

$$U_f \left|x, y\right\rangle = \left|x, y \oplus f(x)\right\rangle, \quad x, y \in \{0,1\}, \tag{22}$$

while a classical fruit-checker can only query U_f as

$$U_f \left|0,0\right\rangle = \left|0, f(0)\right\rangle, \quad U_f \left|0,1\right\rangle = \left|0, f(1)\right\rangle, \quad U_f \left|1,0\right\rangle = \left|1, f(0)\right\rangle, \quad U_f \left|1,1\right\rangle = \left|1, f(1)\right\rangle. \tag{23}$$

The quantum fruit-checker can apply U_f to a linear combination of states in the computational basis. We can show that U_f is unitary.

$$\begin{aligned} \left\langle x^{'}, y^{'} \middle| U_f^{\dagger} U_f \middle| x, y \right\rangle &= \left\langle x^{'}, y^{'} \oplus f(x^{'}) \middle| x, y \oplus f(x) \right\rangle \\ &= \left\langle x^{'} \middle| x \right\rangle \left\langle y^{'} \oplus f(x^{'}) \middle| y \oplus f(x) \right\rangle \\ &= \delta_{x,x'} \delta_{y,y'} \end{aligned} \tag{24}$$

which gives $U_f^{\dagger} U_f = I$.

The Deutsch's algorithm convert the oracle U_f into a phase kickback. Let $\left|y\right\rangle = \left|-\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)$, then

$$U_f \left|x, y\right\rangle = \frac{1}{\sqrt{2}}(\left|x, f(x)\right\rangle - \left|x, 1 \oplus f(x)\right\rangle) = (-1)^{f(x)} \left|x, y\right\rangle. \tag{25}$$

We know that $\left|y\right\rangle = HX \left|0\right\rangle$, then we can write

$$(I \oplus XH) U_f (I \oplus HX) \left|x, 0\right\rangle = (-1)^{f(x)} \left|x, 0\right\rangle. \tag{26}$$

The XH application can be viewed as the uncomputation step. Focusing on the first qubit only, we have

$$\tilde{U}_f \left|x\right\rangle = (-1)^{f(x)} \left|x\right\rangle. \tag{27}$$

The information of $f(x)$ is stored as a phase factor of $\left|x\right\rangle$. The quantum operation for Deutsch's algorithm is as follows:

$$\begin{aligned} \left|0,1\right\rangle &\xrightarrow{H \otimes H} \left|+,-\right\rangle = \frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle) \otimes \left|-\right\rangle \\ &\xrightarrow{U_f} \frac{1}{2}(\left|0\right\rangle (-1)^{f(0)} + \left|1\right\rangle (-1)^{f(1)}) \otimes \left|-\right\rangle \\ &\xrightarrow{H \otimes I} \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)}) \left|0,-\right\rangle + \frac{1}{2}((-1)^{f(0)} - (-1)^{f(1)}) \left|1,-\right\rangle. \end{aligned} \tag{28}$$

We only need one query of U_f to check if the boxes contain the same fruits or not. When we have $f(0) = f(1)$, measuring the first qubit will result in 0 deterministically, and if we have $f(0) \neq f(1)$, then measuring the first qubit will result in 1 deterministically.

2.2 Unstructured search problem

Now we want to find one box with an orange among $N = 2^n$ boxes, and each of other boxes contain an apple. Mathematically, we have a boolean function $f : \{0,1\}^n \to \{0,1\}$, and we want to find one marked x_0 such that $f(x_0) = 1$. In the worst scenario of the classical method, we need to open $N-1$ boxes to get x_0. Using a quantum algorithm known as the Grover's algorithm that relies to an oracle

$$U_f |x, y\rangle = |x, y \oplus f(x)\rangle \,, \quad x \in \{0,1\}^n, y \in \{0,1\}, \tag{29}$$

we can find x_0 with $\mathcal{O}(\sqrt{N})$ queries. The classical probabilistic algorithm can only work on the probability density while the quantum algorithms can work with wavefunction amplitudes, of wich the square results in the probability densities. This is the source of the quadratic speedup of the Grover's algorithm.

The scenario of Grover's algorithm is as follows: we have an initial state which is the uniform superposition of all possible states;

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \,. \tag{30}$$

This superposition can be prepared by using the Hadamard gates on n qubits, as follows:

$$|\psi_0\rangle = H^{\otimes n} |0^n\rangle \,. \tag{31}$$

To find the state $|x_0\rangle$, we would like to amplifiy its wavefunction amplitude from $1/|N\rangle$ to $\sqrt{p} = \Omega(1)$ by using only $\mathcal{O}(\sqrt{N})$ queries to the oracle U_f. By measuring the amplitude-amplified state, we can get an output state $|x\rangle$. To check if $x = x_0$, we apply another query of U_f such that $U_f |x, 0\rangle = |x, f(x)\rangle$. We will get $f(x) = 1$ with probability p. It's still probabilistic, so if we don't get the right x_0 for the first time, we repeat the process. We will obtain x_0 with high probability after $\mathcal{O}(1/p)$ times of repetition.

The first step of the Grover's algorithm is we take $|y\rangle = |-\rangle$ and then we turn the oracle into a phase kickback

$$U_f |x, -\rangle = \frac{1}{\sqrt{2}}(|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle) = (-1)^{f(x)} |x, -\rangle \,. \tag{32}$$

We can decompose any quantum state $|\psi\rangle$ as

$$|\psi\rangle = \alpha |x_0\rangle + \beta |\psi_\perp\rangle \,, \tag{33}$$

where $\langle \psi_\perp | \psi_0 \rangle = 0$. Therefore, we have

$$U_f |\psi\rangle \otimes |-\rangle = -\alpha |x_0\rangle \otimes |-\rangle + \beta |\psi_\perp\rangle \otimes |-\rangle \,. \tag{34}$$

This is because $f(x) = 0$ for x other than x_0. We can discard $|-\rangle$ to obtain an n-qubit unitary

$$R_{x_0}(\alpha |\psi_0\rangle + \beta |\psi_\perp\rangle) = -\alpha |x_0\rangle + \beta |\psi_\perp\rangle \,. \tag{35}$$

Therefore, R_{x_0} is a reflection operator across the hyperplane orthogonal to $|x_0\rangle$ which is known as the Householder reflector

$$R_{x_0} = I - 2 |x_0\rangle \langle x_0| \,. \tag{36}$$

We can write

$$|\psi_0\rangle = \sin(\theta/2) |x_0\rangle + \cos(\theta/2) |\psi_{0\perp}\rangle \,, \tag{37}$$

where $\theta = 2 \sin^{-1} \frac{1}{\sqrt{N}} \approx \frac{2}{\sqrt{N}}$ and $|\psi_{0\perp}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$. Then

$$R_{x_0} |\psi_0\rangle = -\sin(\theta/2) |x_0\rangle + \cos(\theta/2) |\psi_{0\perp}\rangle \,. \tag{38}$$

Thus span$\{|x_0\rangle, |\psi_{0\perp}\rangle\}$ is an invariant subspace of R_{x_0}.

We can consider another Householder reflector,

$$R_{\psi_0} = -(I - 2|\psi_{0\perp}\rangle\langle\psi_{0\perp}|). \tag{39}$$

By using both of the Householder reflectors, we can obtain

$$\begin{aligned} R_{\psi_0}R_{x_0}|\psi_0\rangle &= R_{\psi_0}(|\psi_0\rangle - 2\sin(\theta/2)|x_0\rangle) \\ &= (|\psi_0\rangle - 4\sin^2(\theta/2)|\psi_0\rangle) + 2\sin(\theta/2)|x_0\rangle \\ &= \sin(\theta/2)(3 - 4\sin^2(\theta/2))|\psi_0\rangle + \cos(\theta/2)(1 - 4\sin^2(\theta/2))|\psi_{0\perp}\rangle \\ &= \sin(3\theta/2)|x_0\rangle + \cos(3\theta/2)|\psi_{0\perp}\rangle. \end{aligned} \tag{40}$$

We dub the operator above as the Grover operator G. We can see that it amplifies the amplitude of x_0 from $\sin(\theta/2)$ into $\sin(3\theta/2)$ while decreasing the amplitude of the states orthogonal to $|x_0\rangle$. We can apply G for k times to obtain

$$G^k|\psi_0\rangle = \sin((2k+1)\theta/2)|x_0\rangle + \cos((2k+1)\theta/2)|\psi_{0\perp}\rangle. \tag{41}$$

We want the amplitude of $|x_0\rangle$ as close as 1 as possible. Thus for $\sin(2k+1)\theta/2 \approx 1$, we need $k \approx \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N}$ (because $\theta \approx 2/\sqrt{N}$). This proves that it takes $\mathcal{O}(\sqrt{N})$ queries to find the marked state x_0 by using the Grover's algorithm.

2.3 Amplitude amplification

Another use case of the Grover's algorithm other than the unstructured search is amplitude amplification. Suppose we want to prepare $|\psi_0\rangle$ by using an oracle $U|0^n\rangle = |\psi_0\rangle$ and the $|\psi_0\rangle$ itself is a superposition state as follows:

$$|\psi_0\rangle = \sqrt{p_0}|\psi_{\text{good}}\rangle + \sqrt{1-p_0}|\psi_{\text{bad}}\rangle. \tag{42}$$

We want the state $|\psi_{\text{good}}\rangle$ but cannot obtain it directly, but we have hope to obtain a state that is largely overlap with $|\psi_{\text{good}}\rangle$. In other words, we want to amplify its amplitude.

If we bring this problem into the unstructured search problem, we have $|\psi_{\text{good}}\rangle = |x_0\rangle$ and $p_0 = 1/N$. We don't have access to the answer $|x_0\rangle$ but we assume that we have access to its reflection operator. In this problem, we also assume that we have access to the reflection operator

$$R_{\text{good}} = I - 2|\psi_{\text{good}}\rangle\langle\psi_{\text{good}}|. \tag{43}$$

By using the oracle U_{ψ_0}, we can construct the reflection with respect to the initial state

$$R_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - I = U_{\psi_0}(2|0^n\rangle\langle 0^n| - I)U_{\psi_0}^\dagger. \tag{44}$$

Therefore, we obtain two reflection operators that can be used to construct the Grover operator,

$$G = R_{\psi_0}R_{\text{good}}. \tag{45}$$

We can obtain a state that has $\omega(1)$ overlap with $|\psi_{\text{good}}\rangle$ by applying G^k to $|\psi_0\rangle$ for some $k = \mathcal{O}(1/\sqrt{p_0})$.

2.4 Lower bound of query complexity

The Grover's algorithm can find x_0 with constant probability by making $\mathcal{O}(\sqrt{N})$ times querying R_{x_0}. There has not been any quantum algorithm that can do it fewer than $\Omega(\sqrt{N})$ access to R_{x_0}.

Generally, we can express any quantum search algorithm that starts from an initial state $|\psi_0\rangle$ and queries R_{x_0} for k steps as the following

$$\left|\psi_k^{x_0}\right\rangle = U_k^{x_0}\left|\psi_0\right\rangle = U_k R_{x_0} U_{k-1} R_{x_0} \cdots U_1 R_{x_0}\left|\psi_0\right\rangle, \tag{46}$$

for some unitaries $\{U_i\}$. For simplicity, we can assume that the algorithm does not use any ancilla qubit, as the result can be generalized to the case in the presence of ancilla qubits. The superscipt x_0 indicates that the state depends on the marked state x_0, and solving the search problem means we obtain $\left|\psi_k^{x_0}\right\rangle$ such that

$$|\left\langle\psi_k^{x_0}\middle|x_0\right\rangle|^2 \geq \frac{1}{2}. \tag{47}$$

In other words, we can obtain $|x_0\rangle$ with probability at least $1/2$ by measuring $\left|\psi_k^{x_0}\right\rangle$ in the computational basis. We can prove the queries lower bound of the quantum search algorithm by comparing the action of $U_k^{x_0}$ with a "fake algorithm" with the unitary U_k that can be defined as follows

$$\left|\psi_k\right\rangle = U_k\left|\psi_0\right\rangle = U_k U_{k-1}\cdots U_1\left|\psi_0\right\rangle. \tag{48}$$

We can not obtain the marked state x_0 from this algorithm because its final state $|\psi_k\rangle$ does not contain any information of x_0.

We will use the following discrete l_2-norm

$$||f||_{l_2} = \sqrt{\sum_{x_0\in[N]} ||f^{x_0}||}, \tag{49}$$

for a set of vectors $\{f^{x_0}\}_{x_0\in[N]}$ and each $f^{x_0}\in\mathbb{C}^N$. We also have the following inequality

$$||f||_{l_2} - ||g||_{l_2} \leq ||f+g||_{l_2} \leq ||f||_{l_2} + ||g||_{l_2}. \tag{50}$$

We will prove the lower bound with two steps. The first step is we will show the difference between the true and the fake solution as follows

$$D_k = \sum_{x_0\in[N]} ||\left|\psi_k^{x_0}\right\rangle - \left|\psi_k\right\rangle||^2 = \Omega(N). \tag{51}$$

In the second step, we will prove that

$$D_k \leq 4k^2, \quad k\geq 0, \tag{52}$$

and $D_0 = 0$. Therefore, we must have $k = \Omega(\sqrt{N})$.

In the first step, we can choose a phase factor $e^{i\theta}$ such that

$$\left\langle\psi_k^{x_0}\middle|x_0\right\rangle \geq \frac{1}{\sqrt{2}}. \tag{53}$$

Therefore, using Cauchy-Schwarz inequality, we have

$$||\left|\psi_k^{x_0}\right\rangle - |x_0\rangle||^2 = 2 - 2\left\langle\psi_k^{x_0}\middle|x_0\right\rangle \leq 2-\sqrt{2}. \tag{54}$$

Therefore, we have

$$\sum_{x_0\in[N]} ||\,\left|\psi_k^{x_0}\right\rangle - \left|x_0\right\rangle||^2 \leq 2N - \sqrt{2}N. \tag{55}$$

Meanwhile, from the fake algorithm, we will have

$$\sum_{x_0\in[N]} ||\,\left|\psi_k\right\rangle - \left|x_0\right\rangle||^2 \geq 2N - 2\sum_{x_0\in[N]} |\left\langle x_0|\psi\right\rangle| = 2N - 2\sqrt{N}, \tag{56}$$

which violates the bound in (55). From the two equations above, by using the triangle inequality, we have

$$D_k = \sum_{x_0\in[N]} ||\,\left|\psi_k^{x_0}\right\rangle - \left|\psi_k\right\rangle||^2 = \sum_{x_0\in[N]} ||(\left|\psi_k^{x_0}\right\rangle - \left|x_0\right\rangle) - (\left|\psi_x\right\rangle - \left|x_0\right\rangle)||^2 \tag{57}$$

$$\geq \left(\sqrt{\sum_{x_0\in[N]} ||\,\left|\psi_k\right\rangle - \left|x_0\right\rangle||^2} - \sqrt{\sum_{x_0\in[N]} ||\,\left|\psi_k^{x_0}\right\rangle - \left|x_0\right\rangle||^2}\right)^2 \tag{58}$$

$$\geq (\sqrt{2N - 2\sqrt{N}} - \sqrt{2N - \sqrt{2}N})^2 = \Omega(N). \tag{59}$$

In other words, we found that the true solution and the fake solution must be well seperated in l_2-norm.

3 Quantum Phase Estimation

Let's say we have a unitary U and its eigenvector $\left|\psi\right\rangle$ such that

$$U\left|\psi\right\rangle = e^{2\pi i\theta}\left|\psi\right\rangle, \quad \theta \in [0,1), \tag{60}$$

and we want to find θ to a certain precision. This is a task for quantum phase estimation. Using classical computer, we can estimate θ by using the element-wise division like the following

$$\left\langle j\right| U \left|\psi\right\rangle / \left\langle j|\psi\right\rangle = e^{2\pi i\theta}, \tag{61}$$

for any j in the computational basis. Unfortunately, we cannot implement the element-wise division efficiently on a quantum computer, therefore, we need another algorithm that can work on a quantum computer.

3.1 Hadamard test

Hadamard test is a useful tool for computing the expectation value of a unitary operator with respoect to a state, $\left\langle\psi\right| U \left|\psi\right\rangle$. The unitary U is generally not Hermitian, therefore $\left\langle\psi\right| U \left|\psi\right\rangle$ does not correspond to the measurement of a physical observable and we have to measure the real and imaginary part of the expectation value seperately.

For the real Hadamard test, we have a circuit that does the following operation

$$\begin{aligned} \left|0\right\rangle\left|\psi\right\rangle &\xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)\left|\psi\right\rangle \\ &\xrightarrow{c-U} \frac{1}{\sqrt{2}}(\left|0\right\rangle\left|\psi\right\rangle + \left|1\right\rangle U\left|\psi\right\rangle) \\ &\xrightarrow{H\otimes I} \frac{1}{2}\left|0\right\rangle(\left|\psi\right\rangle + U\left|\psi\right\rangle) + \frac{1}{2}\left|1\right\rangle(\left|\psi\right\rangle - U\left|\psi\right\rangle). \end{aligned} \tag{62}$$

Therefore, the probability of measuring the qubit 0 to be in the state $|0\rangle$ is

$$p(0) = \frac{1}{2}(1 + \mathrm{Re}(\langle\psi| U |\psi\rangle)). \tag{63}$$

The imaginary part of the Hadamard test performs the following operation to $|0\rangle |\psi\rangle$

$$\frac{1}{2} |0\rangle (|\psi\rangle - iU |\psi\rangle) + \frac{1}{2} |1\rangle (|\psi\rangle + iU |\psi\rangle). \tag{64}$$

Therefore, the probability of mesuring the qubit 0 to be in state $|0\rangle$ is

$$p(0) = \frac{1}{2}(1 + \mathrm{Im}(\langle\psi| U |\psi\rangle)). \tag{65}$$

The Hadamard test can be used to estimate θ. For example in the case of real Hadamard test, the probability of measuring the qubit 0 to be in state $|1\rangle$ is

$$p(1) = \frac{1}{2}(1 - \mathrm{Re}(\langle\psi| U |\psi\rangle)) = \frac{1}{2}(1 - \cos(2\pi\theta)), \tag{66}$$

thus

$$\theta = \pm\frac{1}{2\pi} \cos^{-1}(1 - 2p(1)). \tag{67}$$

If we assume that $\theta \approx 0$ and we would like to estimate it to additive precision ϵ, we have

$$p(1) \approx (2\pi\theta)^2 = \mathcal{O}(\epsilon^2). \tag{68}$$

That means, $p(1)$ needs to be estimated to precision $\mathcal{O}(\epsilon^2)$ and the number of samples needed is $\mathcal{O}(1/\epsilon^2)$.

3.2 Kitaev's method for quantum phase estimation

From the previous subsection. we obtain that the number of measurement needed to estimate θ to precision ϵ is $\mathcal{O}(1/\epsilon^2)$. A procedure known as the Kitaev's method can improve the number of measurement quadratically ($\mathcal{O}(1/\epsilon)$).

We assume that the eigenvalue can be exactly represented by using d bits in the fixed point representation

$$\theta = 0.\theta_{d-1}\theta_{d-2} \cdots \theta_0. \tag{69}$$

If $d = 1$, we have $\theta = 0.\theta_0$, where $\theta \in \{0, 1\}$. Then we have $e^{i2\pi\theta} = e^{i\pi\theta_0}$. By using the real Hadamard test, we can obtain that $p(1) = 0$ if $\theta_0 = 0$ and $p(1) = 1$ if $\theta_0 = 1$, whcih is a deterministic result. We only need one measurement of qubit 1 to determine θ_0.

If we consider $\theta = .0 \cdot 0\theta_0$, we need to reach precision $\epsilon < 2^{-d}$ to determine the value of θ_0. This means we need $\mathcal{O}(1/\epsilon^2) = \mathcal{O}(2^{2d})$ repeated measurements or number of queries to U. In the Kitaev's method, we have access to U^j for a suitable power j to reduce the number of queries to U. Specifically, if we can query $U^{2^{d-1}}$, then we have

$$p(1) = \frac{1}{2}(1 - \cos(2\pi.\theta_0)) = \begin{cases} 0, & \text{if } \theta_0 = 0, \\ 1, & \text{if } \theta_0 = 1. \end{cases} \tag{70}$$

The total number of queries of U becomes $\mathcal{O}(2^d)$ and the result is again deterministic.

As we explained above, the Kitaev's method use a more complex quantum circuit with a larger circuit depth to reduce the total number of queries. Instead of estimating θ from a single number, we estimate θ bit-by-bit by assuming access to U^{2j}. This allows us to estimate

$$2^j\theta = \theta_{d-1}\cdots\theta_{d-j}.\theta_{d-j-1}\cdots\theta_0 = .\theta_{d-j-1}\cdots\theta_0 \mod 1. \tag{71}$$

The goal of the algorithm is to estimate the d digits for any θ, and we want to describe and analyze the performance.

First, we can apply the circuit of the real hadamard test with U^{2^j} with $j = 0, 1, \cdots, d-3$ to estimate $p(0)$ fro each j so the error in $2^j\theta$ is less than $1/16$, which means that any perturbation must be due to the 5th digit in the binary representation. We denote the closest 3-bit estimate of α_j mod 1 by β_j. For example, for $2^j\theta = 0.11110$, if $\alpha_j = 0.11101$, then $\beta_j = 0.1111$. But if $\alpha_j = 0.11111$, then $\beta_j = 0.0000$. Another example is if we have $2^j\theta = 0.11101$, if $\alpha_j = 0.11110$, then we have $\beta_j = 0.111$ for rounded down estimation and $\beta_j = 0.000$ for rounded up estimation. We can show that the uncertainty in α_j and β_j is not detrimental to the algorithm.

Then, we can perform some post-processing. Start from $j = d-3$, we can estimate $.\theta_2\theta_1\theta_0$ to accuracy $1/16$. We will proceed with the iteration: for $j = d-4, \cdots, 0$, we assign

$$\theta_{d-j-1} = \begin{cases} 0, & |.0\theta_{d-j-2}\theta_{d-j-3} - \beta_j|_{\text{mod } 1} < 1/4, \\ 1, & |.1\theta_{d-j-2}\theta_{d-j-3} - \beta_j|_{\text{mod } 1} < 1/4. \end{cases} \tag{72}$$

After running the algorithm above, we can recover $\theta = .\theta_{d-1}\cdots\theta_0$ exactly. The number of queries to U is the total cost of Kitaev's method, which is $\mathcal{O}(\sum_{j=0}^{d-3} 2^j) = \mathcal{O}(\epsilon^{-1})$.

For example, we consider $\theta = 0.\theta_4\theta_3\theta_2\theta_1\theta_0 = 0.11111$ with $d = 5$. If we run the Kitaev's algorithm for $j = 0, 1, 2$, we will obtain

j	$2^j\theta$	possible β_j
0	0.11111	$\{0.111, 0.000\}$
1	0.1111	$\{0.111, 0.000\}$
2	0.111	$\{0.111\}$

Start with $j = 2$, we only have one β_j, therefore we can recover $0.\theta_2\theta_1\theta_0 = 0.111$. For $j = 1$, we need to decide θ_3 by using the above equation. If $\beta_j = 0.111$, we have $\theta_3 = 1$, and if $\beta_j = 0.000$, our choice is still $\theta_3 = 1$, since $|.011 - .000|_{\text{mod } 1} = 0.101 = 3/8 > 1/4$ and $|.111 - .000|_{\text{mod } 1} = 0.001 = 1/8 < 1/4$. We can also do the same for $j = 0$, and we can obtain $\theta_4 = 1$, which recovers θ exactly.

References

[1] L. Lin, "Lecture notes on quantum algorithms for scientific computation," *arXiv preprint arXiv:2201.08309*, 2022.