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 $|\psi\rangle \to \left|\psi^{'}\right\rangle \in \mathbb{C}^N$ 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 $\lambda_m$. The measurement of a quantum state by an observable $M$ will always result in one of its eigenvalues $\lambda_m$ 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 $U_{\psi_0}$, 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

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

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

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

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

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

Meanwhile, from the fake algorithm, we will have

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

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

$$\begin{aligned} D_k = \sum_{x_0\in[N]} ||\left|\psi_k^{x_0}\right\rangle - |\psi_k\rangle||^2 &= \sum_{x_0\in[N]} ||(\left|\psi_k^{x_0}\right\rangle - |x_0\rangle) - (|\psi_x\rangle - |x_0\rangle)||^2 && (57)\\ &\geq \left(\sqrt{\sum_{x_0\in[N]} ||\,|\psi_k\rangle - |x_0\rangle\,||^2} - \sqrt{\sum_{x_0\in[N]} ||\left|\psi_k^{x_0}\right\rangle - |x_0\rangle||^2}\right)^2 && (58)\\ &\geq (\sqrt{2N - 2\sqrt{N}} - \sqrt{2N - \sqrt{2}N})^2 = \Omega(N). && (59)\end{aligned}$$

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 $|\psi\rangle$ such that

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

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

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

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, $\langle\psi|U|\psi\rangle$. The unitary $U$ is generally not Hermitian, therefore $\langle\psi|U|\psi\rangle$ 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

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

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

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

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

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

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

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

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 $\epsilon$, 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 $\theta$ to precision $\epsilon$ 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 $\theta_0$.

If we consider $\theta = .0 \cdot 0\theta_0$, we need to reach precision $\epsilon < 2^{-d}$ to determine the value of $\theta_0$. 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 $\theta$ from a single number, we estimate $\theta$ 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 $\theta$, 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 $\alpha_j$ mod 1 by $\beta_j$. 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 $\alpha_j$ and $\beta_j$ 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 $\beta_j$ |
|---|---|---|
| 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 $\beta_j$, therefore we can recover $0.\theta_2\theta_1\theta_0 = 0.111$. For $j = 1$, we need to decide $\theta_3$ 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 $\theta$ exactly.

### 3.3 Quantum Fourier transform

One of the most widely used algorithms in the classical computing is Fourier transform, with its variant, fast Fourier transform, serves as the backbone for many fast algorithms. In quantum computation, the quantum Fourier transform is an important component in many algorithms such as Shor's algorithm and phase estimation. For any $j$ in the computational basis, the discrete forward Fourier transform is defined as

$$U_{\text{FT}} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k\in[N]} e^{i2\pi\frac{kj}{N}} |k\rangle , \tag{73}$$

where in particular,

$$U_{\text{FT}} |0^n\rangle = \frac{1}{\sqrt{N}} \sum_{k\in[N]} |k\rangle = H^{\otimes n} |0^n\rangle . \tag{74}$$

We will use the binary representation of integers

$$k = (k_{n-1} \cdots k_0.), \quad j = (j_{n-1} \cdots j_0.), \tag{75}$$

therefore we have

$$\begin{aligned} \frac{kj}{N} &= k0\frac{j}{2^n} + k_1\frac{j}{2^{n-1}} + \cdots + k_{n-1}\frac{j}{2} \\ &= k_0(.j_{n-1} \cdots j_0) + k_1(j_{n-1}.j_{n-2} \cdots j_0) + \cdots + k_{n-1}(j_{n-1} \cdots j_1.j_0). \end{aligned} \tag{76}$$

The exponential then can be written as

$$e^{i2\pi\frac{kj}{N}} = e^{i2\pi k_0(.j_{n-1}\cdots j_0)}e^{i2\pi k_1(.j_{n-2}\cdots j_0)} \cdots e^{i2\pi k_{n-1}(.j_0)}. \tag{77}$$

We can write the application of the Fourier transform by using the above representation

$$\begin{aligned} U_{\mathrm{FT}} \left|j_{n-1} \cdots j_0\right\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k_{n-1},\cdots,k_0} e^{i2\pi k_0(.j_{n-1}\cdots j_0)}e^{i2\pi k_1(.j_{n-2}\cdots j_0)} \cdots e^{i2\pi k_{n-1}(.j_0)} \left|k_{n-1} \cdots k_0\right\rangle \\ &= \frac{1}{\sqrt{2^n}} \left( \sum_{k_{n-1}} e^{i2\pi k_{n-1}(.j_0)} \left|k_{n-1}\right\rangle \right) \otimes \cdots \otimes \left( \sum_{k_0} e^{i2\pi k_0(.j_{n-1}\cdots j_0)} \left|k_0\right\rangle \right) \\ &= \frac{1}{\sqrt{2}} \Big( \left|0\right\rangle + e^{i2\pi(.j_0)} \left|1\right\rangle \Big) \otimes \Big( \left|0\right\rangle + e^{i2\pi(.j_1 j_0)} \left|1\right\rangle \Big) \otimes \cdots \otimes \Big( \left|0\right\rangle + e^{i2\pi(.j_{n-1}\cdots j_0)} \left|1\right\rangle \Big), \end{aligned} \tag{78}$$

where a series of controlled rotations of the following form is involved

$$\left|0\right\rangle \to \frac{1}{\sqrt{2}} \Big( \left|0\right\rangle + e^{i2\pi(.j_{n-1}\cdots j_0)} \left|1\right\rangle \Big). \tag{79}$$

### 3.4 Quantum phase estimation using quantum Fourier transform

The standard quantum phase estimation (QPE) uses one signal quantum circuit based on QFT and requires $d$-ancilla qubits to store the phase information in the quantum computer. We define a controlled unitary operation

$$U = \sum_{j \in [2^d]} \left|j\right\rangle \left\langle j\right| \otimes U^j, \tag{80}$$

Thus, when $d = 1$, $U$ is just a controlled $U$ operation. It seems that we need to implement all $2^d$ different $U^j$ in general. However, this is not necessary. If we use the binary representation of integers $j = (j_{d-1} \cdots j_0.) = \sum_{i=0}^{d-1} j_i 2^i$, we have $U^j = U^{\sum_{i=0}^{d-1} j_i 2^i} = \Pi_{i=0}^{d-1} U^{j_i 2^i}$. Therefore, we have

$$\begin{aligned}
\mathcal{U} &= \sum_{j \in [2^d]} |j\rangle \langle j| \otimes U^j \\
&= \sum_{j_{d-1}, \cdots, j_0} (|j_{d-1}\rangle \langle j_{d-1}|) \otimes \cdots \otimes (|j_0\rangle \langle j_0|) \otimes \prod_{i=0}^{d-1} U^{j_i 2^i} \\
&= \prod_{i=0}^{d-1'} \left( \sum_{j_i} |j_i\rangle \langle j_i| \otimes U^{j_i 2_i} \right) \\
&= \prod_{i=0}^{d-1'} \left( |0\rangle \langle 0| \otimes I_n + |1\rangle \langle 1| \otimes U^{2^i} \right). \qquad (81)
\end{aligned}$$

Let the initial state in the ancilla qubits to be $|0^n\rangle$ that we transform according to

$$\left|0^d\right\rangle |\psi_0\rangle \xrightarrow{U_{\mathrm{FT}} \otimes I} \frac{1}{\sqrt{2^d}} \sum_{j \in [2^d]} |j\rangle |\psi_0\rangle \qquad (82)$$

$$\xrightarrow{\mathcal{U}} \frac{1}{\sqrt{2^d}} \sum_{j \in [2^d]} (|j\rangle \otimes U^j |\psi_0\rangle) = \frac{1}{\sqrt{2^d}} \sum_{j \in [2^d]} |j\rangle e^{i2\pi\phi j} |\psi_0\rangle$$

$$\xrightarrow{U_{\mathrm{FT}}^\dagger \otimes I} \sum_{k' \in [2^d]} \left( \frac{1}{2^d} \sum_{j \in [2^d]} e^{i2\pi j \left(\theta - \frac{k'}{2^d}\right)} \right) \left|k'\right\rangle |\psi_0\rangle \qquad (83)$$

where we have $\theta = \frac{k}{2^d}$ for some $k \in [2^d]$. We can obtain the phase information by measuring the ancilla qubits, where we will obtain the state $|k\, |\psi_0\rangle\rangle$ with certainty.

### 3.5 Analysis of quantum phase estimation

The QPE algorithms assume the following:

1. $|\psi_0\rangle$ is an eigenstate
2. $\theta_0$ has a $d$-bit binary representation.

Practically, neither condition can be exactly satisfied, that's why we need to analyze the effect on the error of the QPE. We will assume the only sources of errors are at the mathematical level, for example due to an inexact eigenstate $|\psi\rangle$ or Monte Carlo errors in the readout process due to the probabilistic nature of the measuremnet process. We will study what happens when the conditions are not met. First, we assume that $U$ has the eigendecomposition

$$U |\psi_j\rangle = e^{i2\pi\theta_j} |\psi_j\rangle. \qquad (84)$$

Without loss of generality, we assume $0 \leq \theta_0 \leq \theta_1 \cdots \leq \theta_{N-1} \leq 1$, and we are interested to find $\theta_0$.

First, we will assume that $\theta_i$'s have an exact $d$-bit binary representation and the quantum state is given by a linear combination

$$|\psi_0\rangle = \sum_{k=0}^{N-1} c_k |\psi_k\rangle. \qquad (85)$$

The overlap is $p_0 = |\langle\psi|\phi_0\rangle|^2 = |c_0| < 1$. If we apply the QPE operation as in Equation (82) to $\left|0^t\right\rangle|\phi\rangle$, with $t = d$, and measure the ancilla qubits, we can obtain the eigenstate $|\psi_0\rangle$ and the binary representation of $\theta_0$ with probability $p_0$. It is obvious that in order to recognize that $\theta_0$ is the desired phase, we need some priori knowledge about $\theta_0$, for example, $\theta_0 \in (a, b)$ and $\theta_1 > b$ for all $i \neq 0$.

For simplicity, we focus on the case where only the condition 2 is violated, that is, we need to apply the QPE circuit to an initial state $\left|0^t\right\rangle|\phi\rangle$ with $t > d$. After applying the QPE circuit, we will obtain

$$\begin{aligned}\left|0^t\right\rangle|\psi_0\rangle &\to \sum_{k'\in[T]}\left(\frac{1}{T}\sum_{j\in[T]} e^{i2\pi j\left(\theta_0-\frac{k'}{T}\right)}\right)\left|k'\right\rangle|\psi_0\rangle \\ &= \sum_{k'}\gamma_{0,k'}\left|k'\right\rangle|\psi_0\rangle, \end{aligned} \tag{86}$$

where

$$\gamma_{0,k'} = \frac{1}{T}\sum_{j\in[T]} e^{i2\pi j\left(\theta_0-\frac{k'}{T}\right)} = \frac{1}{T}\frac{1-e^{i2\pi T(\theta_0-\tilde{\theta}_{k'})}}{1-e^{i2\pi(\theta_0-\tilde{\theta}_{k'})}}. \quad \tilde{\theta}_{k'} = \frac{k'}{T}. \tag{87}$$

If $\theta_0$ has an exact $d$-bit representation, $\theta_0 = \tilde{\theta}_{k_0'}$ for some $k_0'$, then $\gamma_{0,k'} = \delta_{k',k_0'}$

Now we assume that $\theta_0 \neq \tilde{\theta}_{k'}$ for any $k'$. in terms of the phase, we want to find $k_0'$ such that

$$|\theta_0 - \tilde{\theta}_{k_0'}|_1 \leq \epsilon, \tag{88}$$

where $\epsilon = 2^{-d}$ is the precision parameter. In particular, for any $k'$ we have

$$|\theta_0 - \tilde{\theta}_{k'}| \leq 1/2/ \tag{89}$$

By using the relation for any $\alpha \in [-\pi, \pi]$,

$$|1-e^{i\alpha}| = \sqrt{2(1-\cos\alpha)} = 2|\sin(\alpha/2)| \geq \frac{2}{\pi}|\alpha| \tag{90}$$

therefore, we obtain

$$|\gamma_{0,k'}| \leq \frac{2}{T\frac{2}{\pi}2\pi|\theta_0-\tilde{\theta}_{k'}|_1} = \frac{1}{2T|\theta_0-\tilde{\theta}_{k'}|_1}. \tag{91}$$

Let $k_0'$ be the random measurement outcome. We can calculate the probability of obtaining some $\tilde{\theta}_{k_0'}$ that is at least $\epsilon$ distance away from $\theta_0$ as the following

$$\begin{aligned} P(|\theta_0-\tilde{\theta}_{k_0'}|_1 \geq \epsilon) &= \sum_{|\theta_0-\tilde{\theta}_{k'}|_1\geq\epsilon}|\gamma_{0,k'}|^2 \\ &\leq \sum_{|\theta_0-\tilde{\theta}_{k'}|_1\geq\epsilon}\frac{1}{4T^2|\theta-\tilde{\theta}_{k'}|_1^2} \\ &\leq \frac{1}{4T^2}\int_{\epsilon}^{\infty}\frac{1}{x^2}dx + \frac{2}{4T^2\epsilon^2}. \end{aligned} \tag{92}$$

Let us set $t-d = \log_2\delta^{-1}$, then we have $T\epsilon = 2^{t-d} \geq \delta^{-1}$. Thus for $0 < \delta < 1$, the failure probability is

$$P(|\theta_0-\tilde{\theta}_{k_0'}|_1 \geq \epsilon) \leq \delta. \tag{93}$$

Therefore, if we want to obtain the phase $\theta_0$ to accuracy $\epsilon = 2^{-d}$ with a success probability at least $1-\delta$, we need $d + \log_2 \delta^{-1}$ ancilla qubits to store the value of the phase and the simulation time needs to be $T = (\epsilon\delta)^{-1}$.

# 4 Applications of quantum phase estimation

## 4.1 Ground state energy estimation

Let $H$ be a Hermitian matrix that describes a system. This matrix is known as the Hamiltonian, and below are two examples of it

### Transverse field Ising model

The Hamiltonian for the one dimensional TFIM with nearest neighbor interaction of length $n$ is

$$H = \sum_{i=1}^{n-1} Z_i Z_{i+1} - g \sum_{i=1}^{n} X_i, \tag{94}$$

which has the dimension of $2^n$.

### Fermionic system in second quantization

For a fermionic system such as electrons, the Hamiltonian can be expressed in terms of the creation and annihilation operators as follows

$$H = \sum_{ij=1}^{n} T_{ij} \hat{a}_i^\dagger \hat{a}_j + \sum_{ijkl=1}^{n} V_{ijkl} \hat{a}_i^\dagger \hat{a}_j^\dagger \hat{a}_k \hat{a}_l. \tag{95}$$

A transformation called Jordan-Wigner transformation can convert the creation and annihilation operators into the Pauli operators

$$\hat{a}_i = Z^{\otimes(i-1)} \otimes \frac{1}{2}(X+iY) \otimes I^{\otimes(N-i)}, \quad \hat{a}_i^\dagger = Z^{\otimes(i-1)} \otimes \frac{1}{2}(X-iY) \otimes I^{\otimes(N-i)}. \tag{96}$$

The dimension of the Hamiltonian matrix $\hat{H}$ is also $2^n$. We can define the number operator $\hat{n}_i$

$$\hat{n}_i = \hat{a}_i^\dagger \hat{a}_i = \frac{1}{2}(I - Z_i). \tag{97}$$

This number operator can define the total number of particles in the system,

$$N_e = \langle\psi| \sum_{i=1}^{n} \hat{n}_i |\psi\rangle . \tag{98}$$

The total number of particles is conserved by the Hamiltonian.

The Hamiltoniaian has the eigendecomposition as follows:

$$H |\psi_j\rangle = \lambda_j |\psi_j\rangle . \tag{99}$$

# 5 Block encoding

To perform the matrix computation in quantum computers, we have to access the information from the matrix, $A \in \mathbb{C}^{N\times N}$ $(N = 2^n)$, which is generally not unitary. Another possible way is to convert the non-unitary matrix into the unitary one, $e^{i\tau A}$. This is useful if $e^{i\tau A}$ can be constructed by using simple circuits.

A more general way to input the information is by block-encoding. A dense matrtix $A$ without an obvious structure will be expensive according to the size of the input (for example, exponential in $n$). Therefore, the input is usually assumed to be $s$-sparse, which contains at most $s$ non-zero elements in each row or column. The block-encoding procedure provides a way to locate the nonzero entries of a block-encoded matrix. However, this might also be a difficult task if the number of the non-zero entries in the matrix is the exponential of $n$.

## 5.1 Query model for matrix entries

The matrix $A$ is assumed to be an $n$-qubit, square-matrix, with

$$||A||_{\text{max}} = \max_{i,j} |A_{ij}| < 1. \tag{100}$$

If not, then we rescale the matrix $A$ to be $\tilde{A}/\alpha$ for some $\alpha > ||A||_{\text{max}}$. To query the entry of this matrix, we assume an oracle that can do the following operation

$$O_A |0\rangle |i\rangle |j\rangle = (A_{ij} |0\rangle + \sqrt{1 - |A_{ij}|^2} |1\rangle) |i\rangle |j\rangle . \tag{101}$$

The above oracle works like a controlled rotation, where $|i\rangle , |j\rangle$ are the control qubits and $|0\rangle$ is the signal qubit as the target. The controlled rotation will encode $A_{ij}$ as the amplitude of $|0\rangle$.

The classical information in $A$ is typically not stored in the oracle $O_A$, and it is more natural to express the oracle as

$$\tilde{O}_A |0\rangle |i\rangle |j\rangle = \left|\tilde{A}_{ij}\right\rangle |i\rangle |j\rangle , \tag{102}$$

where the fixed-point representation $\tilde{A}_{ij}$ is either computed on the fly by the quantum computer or obtained through an external database.

## 5.2 Block-encoding

Assume we can find an $(n+1)$-qubit unitary matrix $U$ such that

$$U_A = \begin{bmatrix} A & * \\ * & * \end{bmatrix} \tag{103}$$

where $*$ is irrelevant. Then for any $n$-qubit $|b\rangle$ such that

$$|0, b\rangle = \begin{bmatrix} b \\ 0 \end{bmatrix} , \tag{104}$$

we have

$$U_A |0, b\rangle = |0\rangle A |b\rangle + |\perp\rangle . \tag{105}$$

To obtain $A |b\rangle$, we need to measure the qubit 0 and only keep the state if it returns 0. The success probability of this measurement can be computed as follows

$$p(0) = ||A |b\rangle ||^2 = \langle b| A^\dagger A |b\rangle . \tag{106}$$

Here, we see that the success probability only depends on $A$ and $|b\rangle$. The other elements in $U_A$ is irrelevant. The matrix $U_A$ can be generalized into an $(n+m)$-qubit matrix . To get $A$, we can compute the following

$$A = (\langle 0^m| \otimes I_n) U_A (|0^m\rangle \otimes I_n). \tag{107}$$

It is difficult to block encode $A$ exactly. A block encoding unitary $U_A$ typically can only block encode $A$ with some error $\epsilon$. Therefore, given an $n$-qubit matrix $A$, and $\alpha, \epsilon \in \mathbb{R}_+$, the $U_A$ is an $(\alpha, m, \epsilon)$-block-encoding of $A$ if

$$||A - \alpha(\langle 0^m| \otimes I_n) U_A (|0^m\rangle \otimes I_n)|| \leq \epsilon. \tag{108}$$

When the block-encoding is exact, $\epsilon = 0$, we call it as $(\alpha, m)$-block-encoding of $A$. The set of all $(\alpha, m, \epsilon)$-block-encoding of $A$ is denoted as $\mathrm{BE}_{\alpha,m}(A, \epsilon)$ and we define $\mathrm{BE}_{\alpha,m}(A) = \mathrm{BE}(A, 0)$

Assume we know each entry of $n$-qubit matrix $A$. GIven an $(m+n)$-qubit unitary $U_A$, we can verify that $U_A \in \mathrm{BE}_{1,m}(A)$ by verifying that

$$\langle 0^m, i| U_A |0^m, j\rangle = A_{ij}. \tag{109}$$

We can first evaluate the state $U_A |0^m, j\rangle$ and perform inner product with $|0^m, i\rangle$. If the ancilla qubits are measured to be $0^m$, the system qubits return the normalized state $\sum_i A_{ij} |i\rangle / || \sum_i A_{ij} |i\rangle ||$.

## 6 Matrix functions of Hermitian matrices

Let $A$ an $n$-qubit Hermitian matrix with eigenvalue decomposition

$$A = V \Lambda V^\dagger \tag{110}$$

where $\Lambda = \mathrm{diag}(\{\lambda_1\})$ is a diagonal matrix and $\lambda_0 \leq \cdots \leq \lambda_{N-1}$. Let the scalar function $f$ be well defined on all $\lambda_i$'s. Then the matrix function $f(A)$ can be defined in terms of the eigendecompositon

$$f(A) = V f(\Lambda) V^\dagger. \tag{111}$$

### 6.1 Qubitization of Hermitian matrices with hermitian block encoding

We introduce some heuristic idea behind qubitization. For any $-1 < \lambda \leq 1$, we can consider a $2 \times 2$ matrix

$$O(\lambda) = \begin{bmatrix} \lambda & -\sqrt{1-\lambda^2} \\ \sqrt{1-\lambda^2} & \lambda \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \tag{112}$$

From this, we have

$$O^k(\lambda) = \begin{bmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{bmatrix}. \tag{113}$$

using the first and second kind of Chebyshev polynomials,

$$T_k(\lambda) = \cos(k\theta), \quad U_{k-1}(\lambda) = \frac{\sin(k\theta)}{\sin\theta} = \frac{\sin(k\theta)}{\sqrt{1-\lambda^2}}, \tag{114}$$

we have

$$O^k(\lambda) = \begin{bmatrix} T_k(\lambda) & -\sqrt{1-\lambda^2} U_{k-1}(\lambda) \\ \sqrt{1-\lambda^2} U_{k-1}(\lambda) & T_k(\lambda) \end{bmatrix}. \tag{115}$$

In the simplest scenario, we assume that $U_A = \mathrm{HBE}_{1,m}(A)$, where $A$ has spectral decomposition as follows

$$A = \sum_i \lambda_i \left|v_i\right\rangle \left\langle v_i\right| . \tag{116}$$

For each eigenstate $\left|v_i\right\rangle$, we have

$$U_A \left|0^m\right\rangle \left|v_i\right\rangle = \left|0^m\right\rangle A \left|v_i\right\rangle + \left|\tilde{\perp}\right\rangle , \tag{117}$$

where

$$\Pi \left|\tilde{\perp}\right\rangle = (\left|0^m\right\rangle \left\langle 0^m\right| \otimes I_n) \left|\tilde{\perp}\right\rangle = 0. \tag{118}$$

Also, we can write

$$\left|\tilde{\perp}_i\right\rangle = \sqrt{1-\lambda_i^2} \left|\perp_i\right\rangle , \tag{119}$$

where $\left|\perp_i\right\rangle$ is a normalized state.

If $\lambda_i = \pm 1$, then $\mathcal{H} = \mathrm{span}\{\left|0^m\right\rangle \left|v_i\right\rangle\}$ is already an invariant subspace of $U_A$. By using the fact that $U_A U_A^\dagger = I$, we have

$$U_A \left|\perp_i\right\rangle = \sqrt{1-\lambda_i^2} \left|0^m\right\rangle \left|v_i\right\rangle - \lambda_i \left|\perp_i\right\rangle . \tag{120}$$

# References

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