

# 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

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

that has a Hermitian conjugate which is

$$\psi^\dagger = [\psi_0^* \quad \psi_1^* \quad \cdot \quad \cdot \quad \psi_{N-1}^*]. \quad (2)$$

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

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

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

$$\langle i|\phi\rangle \langle\psi|j\rangle = \langle i|\phi\rangle \langle\psi|j\rangle. \quad (4)$$

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

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

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

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

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

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

where  $0 \leq \theta < \pi$ ,  $0 \leq \phi < 2\pi$ . 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

$$a = (\sin \theta \cos \psi, \sin \theta \sin \psi, \cos \theta)^T. \quad (8)$$

### 1.1.2 Quantum operator postulate

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

$$|\psi'\rangle = U |\psi\rangle. \quad (9)$$

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

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

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

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

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

$$|\psi(t_2)\rangle = U(t_2, t_1) |\psi(t_1)\rangle. \quad (12)$$

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

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

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

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

### 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

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

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

$$p(m) = \langle \psi | P_m | \psi \rangle. \quad (16)$$

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

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

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

$$\sum_m P_m = I \implies \sum_m p_m = \sum_m \langle \psi | P_m | \psi \rangle = 1. \quad (18)$$

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

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

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

$$X |\pm\rangle = \lambda_\pm |\pm\rangle, \quad (20)$$

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  $M$ ,

$$M = X = |+\rangle \langle +| - |-\rangle \langle -|. \quad (21)$$

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  $f : \{0, 1\} \rightarrow$

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

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

while a classical fruit-checker can only query  $U_f$  as

$$U_f |0, 0\rangle = |0, f(0)\rangle, \quad U_f |0, 1\rangle = |0, f(1)\rangle, \quad U_f |1, 0\rangle = |1, f(0)\rangle, \quad U_f |1, 1\rangle = |1, f(1)\rangle. \quad (23)$$

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.

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

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

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

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

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

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

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

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

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

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

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  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , 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

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

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 which 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;

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \quad (30)$$

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

$$|\psi_0\rangle = H^{\otimes n} |0^n\rangle. \quad (31)$$

To find the state  $|x_0\rangle$ , we would like to amplify its wavefunction amplitude from  $1/\sqrt{N}$  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

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

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

$$|\psi\rangle = \alpha |x_0\rangle + \beta |\psi_\perp\rangle, \quad (33)$$

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

$$U_f |\psi\rangle \otimes |-\rangle = -\alpha |x_0\rangle \otimes |-\rangle + \beta |\psi_\perp\rangle \otimes |-\rangle. \quad (34)$$

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

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

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

$$R_{x_0} = I - 2 |x_0\rangle \langle x_0|. \quad (36)$$

We can write

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

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

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

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

We can consider another Householder reflector,

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

By using both of the Householder reflectors, we can obtain

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

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

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

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.

## References

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