Lecture 3

Definition 9 (Quantum query algorithm). *A quantum query algorithm of depth d is specified by the following data:*

1. $w \in \mathbb{N}$. *(Dimension of the workspace, i.e., non-query, part of the algorithm.)*
2. $d+1$ *unitary matrices* $U_0, U_1, \ldots, U_d \in \mathbb{C}^n \otimes \mathbb{C}^m \otimes \mathbb{C}^w = \mathbb{C}^{nmw}$.
3. *A* Γ*-outcome projective measurement* $\mathcal{M} := \{\Pi_s \mid s \in \Gamma\}$ *on* $\mathbb{C}^{nmw}$.

Definition 10 (Quantum oracle). *For $x \in \{0, \ldots, m-1\}^n$, the quantum oracle of x is the unitary matrix $O_x \in \mathbb{C}^{nm \times nm}$ defined by*

$$O_x \left|i\right\rangle \left|j\right\rangle = \left|i\right\rangle \left|j + x_{i+1} \mod m\right\rangle, \tag{24}$$

for all $i \in \{0, 1, \ldots, n-1\}$ and $j \in \{0, \ldots, m-1\}$. (And linearly extended. $\mod m$ maps integers to the range $\{0, \ldots, m-1\}$)

In the special case where $m = 2$, this is the same as

$$O_x \left|i\right\rangle \left|b\right\rangle = \left|i\right\rangle \left|b \oplus x_{i+1}\right\rangle, \tag{25}$$

for all $i \in \{0, 1, \ldots, n-1\}$ and $b \in \{0, 1\}$, where $\oplus$ denotes XOR and $\left|b\right\rangle$ represents a 1-qubit quantum state.

Definition 11 (Quantum query computation). *Given $x \in D$ and a quantum query algorithm $\mathcal{A}$, we write $\mathcal{A}(x)$ for the random variable on $\{0, 1\}$ defined by, for all $i \in \Gamma$*

$$\Pr[\mathcal{A}(x) = i] := \|\Pi_i \cdot U_d(O_x \otimes \mathbb{1}_w) \ldots U_1(O_x \otimes \mathbb{1}_w) U_0 \left|0\right\rangle\|^2, \tag{26}$$

where $\mathbb{1}_w \in \mathbb{C}^{w \times w}$ is the identity matrix and we recall $\left|0\right\rangle \in \mathbb{C}^{nmw}$ is the first computational basis vector. (Note there are d occurrences of O_x on the RHS.)

Comment: Draw the circuit note that the tensored identity is not drawn.

Let $\epsilon \in (0, 1/2)$. We say that a quantum query algorithm $\mathcal{A}$ computes f with (two-sided) bounded-error ϵ if

$$\forall x \in D, \Pr[\mathcal{A}(x) = f(x)] \geq 1 - \epsilon, \tag{27}$$

where the probability is over the random variable $\mathcal{A}(x)$.

Definition 12 (Quantum query complexity). *For $\epsilon \in (0, 1/2)$, $Q_\epsilon(f)$ is defined to be the minimum depth of any quantum query algorithm that computes f with (two-sided) bounded-error ϵ. Also standard to write $Q(f) = Q_{1/3}(f)$.*

Grover's algorithm. Recall

$$\mathrm{OR}_n \colon \{0, 1\}^n \to \{0, 1\}. \tag{28}$$

It will be convenient to work with an alternative form of the quantum oracle.

Definition 13 (Quantum phase oracle). *For $x \in \{0, 1\}^n$ the quantum phase oracle of x is the unitary matrix $U_x \in \mathbb{C}^{2n \times 2n}$ defined by*

$$U_x \left|i\right\rangle \left|b\right\rangle = (-1)^{x_{i+1} \cdot b} \left|i\right\rangle \left|b\right\rangle. \tag{29}$$

Let

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{30}$$

denote the Hadamard matrix.

(Quantum query complexity does not change regardless of whether we use the phase oracle or the normal oracle.)

Lemma 1 (Phase kickback trick). *For all $x \in \{0, 1\}^n$, $U_x = (\mathbb{1}_n \otimes H) O_x (\mathbb{1}_n \otimes H)$. Moreover, since $H^2 = \mathbb{1}_2$, we also have $O_x = (\mathbb{1}_n \otimes H) U_x (\mathbb{1}_n \otimes H)$.*

Note that the quantum phase oracle of x can be implemented using one call to the quantum oracle of x together with unitaries *independent* of x, and vice versa. Therefore, if we defined quantum query complexity using the quantum phase oracle instead of the quantum oracle, the value of quantum query complexity would not change.

Proof. Note that for $b \in \{0, 1\}$, we have

$$H \left|b\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + (-1)^b \left|1\right\rangle). \tag{31}$$

Then

$$
\begin{aligned}
|i\rangle |b\rangle &\overset{\mathbb{1}_n \otimes H}{\mapsto} |i\rangle \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b |1\rangle) \overset{O_x}{\mapsto} \frac{1}{\sqrt{2}} |i\rangle (|x_{i+1}\rangle + (-1)^b |x_{i+1} \oplus 1\rangle) \\
&\overset{\mathbb{1}_n \otimes H}{\mapsto} \frac{1}{\sqrt{2}} |i\rangle (\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_{i+1}} |1\rangle) + (-1)^b \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_{i+1} \oplus 1} |1\rangle)) \\
&= \frac{1}{2} |i\rangle ((1 + (-1)^b) |0\rangle + (-1)^{x_{i+1}} |1\rangle) + (-1)^{x_{i+1}}(1 - (-1)^b) |1\rangle) \\
&= (-1)^{x_{i+1} \cdot b} |i\rangle |b\rangle ,
\end{aligned}
$$

as required. □

Remark 3. *There is a generalization of the quantum phase oracle definition for $m > 2$ (codmain of the function is $\{0, 1, \ldots, m-1\}$) — see Andrew Childs' lecture notes, Section 20.2.*

For $t \in \mathbb{N}$, define $\mathrm{OR}_n^{0,t}$ to be OR_n with the restricted domain $D_{0,t} \coloneqq \{x \in \{0,1\}^n \mid |x| \in \{0, t\}\}$.

Proposition 3 (Grover's algorithm)**.** *For all $n, t \in \mathbb{N}$ with $t \leq n/3$,*

$$
Q(\mathrm{OR}_n^{0,t}) \leq \frac{\pi}{4}\sqrt{\frac{n}{t}} + \frac{1}{2}. \tag{32}
$$

Proof. Let $|\psi\rangle$ denote the n-dimensional quantum state

$$
|\psi\rangle \coloneqq \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle , \tag{33}
$$

and let $G \in \mathbb{C}^{n \times n}$ denote the following unitary matrix

$$
G \coloneqq \mathbb{1}_n - 2|\psi\rangle\langle\psi|. \tag{34}
$$

For $x \in \{0,1\}^n$, let

$$
V_x \coloneqq \sum_{i=0}^{n-1} (-1)^{x_{i+1}} |i\rangle\langle i| = \mathbb{1}_n - 2 \sum_{i | x_{i+1} = 1} |i\rangle\langle i|. \tag{35}
$$

(V_x can be instantiated using the quantum phase oracle with b set to 1, and still uses 1 call to O_x.)

Let

$$
\Pi_0 \coloneqq |\psi\rangle\langle\psi| \quad \text{and} \quad \Pi_1 \coloneqq \mathbb{1}_n - \Pi_0. \tag{36}
$$

Clearly, $\{\Pi_0, \Pi_1\}$ defines a $\{0,1\}$-outcome measurement on $\mathbb{C}^n$.

For $k \in \mathbb{N}$, we now consider the following quantity, which can be seen as the probability that a k-query quantum algorithm outputs 0:

$$
p_x \coloneqq \| \Pi_0 (G V_x)^k |\psi\rangle \|^2. \tag{37}
$$

Two cases:

1. $x = 0^n$. In this case $V_x = \mathbb{1}_n$ and $G^k |\psi\rangle = (-1)^k |\psi\rangle$ so $p_x = 1$.
2. $|x| = t$. Define the following orthogonal quantum states:

$$
|\psi_0\rangle \coloneqq \frac{1}{\sqrt{n-t}} \sum_{i | x_{i+1} = 0} |i\rangle , \tag{38}
$$

$$
|\psi_1\rangle \coloneqq \frac{1}{\sqrt{t}} \sum_{i | x_{i+1} = 1} |i\rangle . \tag{39}
$$

Then

$$
|\psi\rangle = \sqrt{1 - \frac{t}{n}} |\psi_0\rangle + \sqrt{\frac{t}{n}} |\psi_1\rangle = \cos(\theta) |\psi_0\rangle + \sin(\theta) |\psi_1\rangle , \tag{40}
$$

where $\theta \coloneqq \arcsin(\sqrt{t/n}) \in (0, \pi/2]$.

We have

$$GV_x |\psi_0\rangle = G |\psi_0\rangle = |\psi_0\rangle - 2\cos(\theta) |\psi\rangle = (1 - 2\cos^2(\theta)) |\psi_0\rangle - 2\cos(\theta)\sin(\theta) |\psi_1\rangle = -\cos(2\theta) |\psi_0\rangle - \sin(2\theta) |\psi_1\rangle . \tag{41}$$

$$GV_x |\psi_1\rangle = -G |\psi_1\rangle = -|\psi_1\rangle + 2\sin(\theta) |\psi\rangle = 2\sin(\theta)\cos(\theta) |\psi_0\rangle + (2\sin^2(\theta) - 1) |\psi_1\rangle = \sin(2\theta) |\psi_0\rangle - \cos(2\theta) |\psi_1\rangle . \tag{42}$$

Therefore, GV_x applied to the state $|\psi\rangle$ always stays in the 2-dimensional subspace $\mathrm{span}(|\psi_0\rangle, |\psi_1\rangle) \leq \mathbb{C}^n$. Therefore, we can reduce the analysis to linear algebra in $\mathbb{C}^2$ by working in the basis $|\psi_0\rangle, |\psi_1\rangle$. In this basis, $|\psi\rangle$ is represented as

$$\begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix}, \tag{43}$$

and $-GV_x$ is represented as

$$A := \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}. \tag{44}$$

This is rotation matrix by angle 2θ anticlockwise. Therefore

$$A^k = \begin{pmatrix} \cos(2k\theta) & -\sin(2k\theta) \\ \sin(2k\theta) & \cos(2k\theta) \end{pmatrix}. \tag{45}$$

(This is geometric intuitive, but can also prove this rigorously by diagonalizing A and then taking the kth power, as in the first homework.)

Therefore,

$$A^k \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix} = \begin{pmatrix} \cos(2k\theta)\cos(\theta) - \sin(2k\theta)\sin(\theta) \\ \sin(2k\theta)\cos(\theta) + \cos(2k\theta)\sin(\theta) \end{pmatrix} = \begin{pmatrix} \cos((2k+1)\theta) \\ \sin((2k+1)\theta) \end{pmatrix}. \tag{46}$$

Therefore,

$$(GV_x)^k |\psi\rangle = (-1)^k (\cos((2k+1)\theta) |\psi_0\rangle + \sin((2k+1)\theta) |\psi_1\rangle). \tag{47}$$

Therefore,

$$p_x = [\cos(\theta)\cos((2k+1)\theta) + \sin(\theta)\sin((2k+1)\theta)]^2 = \cos^2(2k\theta).$$

Let $r := \frac{\pi}{4\theta}$ and $k := \lfloor r \rceil \in [r - 1/2, r + 1/2]$ (where $\lfloor \cdot \rceil$ denotes rounding to the nearest integer). Then

$$\begin{aligned} p_x = \cos^2(2k\theta) &\leq \cos^2(2(r - 1/2)\theta) && \text{(to see the } \leq \text{, draw } \cos^2(A) \text{ around } A = \pi/2) && (48) \\ &= \cos^2(\pi/2 - \theta) = \sin^2(\theta) = \frac{t}{n} \leq 1/3. && \text{(last } \leq \text{ by proposition conditions)} && (49) \end{aligned}$$

Therefore,

$$Q(\mathrm{OR}_n^{0,t}) \leq k := \lfloor \frac{\pi}{4\theta} \rceil \leq \frac{\pi}{4\theta} + \frac{1}{2} = \frac{\pi}{4\arcsin(\sqrt{t/n})} + \frac{1}{2} \leq \frac{\pi}{4}\sqrt{\frac{n}{t}} + \frac{1}{2}, \tag{50}$$

where the last inequality uses $\arcsin(a) \geq a$ for all $a \in [0, 1]$.

□