

Proof sketches

1 Lecture 1

Lemma 1.1. $\| |\psi_0^0\rangle - |\psi_i^0\rangle \| = 0$

Proof. $|\psi_0^0\rangle = |\psi_i^0\rangle = U_0|0, 0\rangle$ □

Lemma 1.2. $\| |\psi_0^T\rangle - |\psi_i^T\rangle \| \geq 1/3$ if the algorithm succeeds w.p. $\geq 2/3$ after T queries

Proof. Success conditions: $\|(\text{Id} \otimes |0\rangle\langle 0|)|\psi_0^T\rangle\|^2 \geq 2/3$ and $\|(\text{Id} \otimes |1\rangle\langle 1|)|\psi_i^T\rangle\|^2 \geq 2/3$

$$\begin{aligned}
 \| |\psi_0^T\rangle - |\psi_i^T\rangle \|^2 &= 2(1 - \text{Re}(\langle \psi_0^T | \psi_i^T \rangle)) \\
 &= 2(1 - \text{Re}(\langle \psi_0^T | (\text{Id} \otimes |0\rangle\langle 0|) |\psi_i^T\rangle) - \text{Re}(\langle \psi_0^T | (\text{Id} \otimes |1\rangle\langle 1|) |\psi_i^T\rangle)) \\
 &\geq 2(1 - \|(\text{Id} \otimes |0\rangle\langle 0|)\psi_0^T\| \cdot \|(\text{Id} \otimes |0\rangle\langle 0|)\psi_i^T\| - \|(\text{Id} \otimes |1\rangle\langle 1|)\psi_0^T\| \cdot \|(\text{Id} \otimes |1\rangle\langle 1|)\psi_i^T\|) \\
 &\hspace{15em} \text{by Cauchy-Schwarz inequality} \\
 &\geq 2(1 - 2\sqrt{2}/3) \hspace{15em} \text{by success conditions} \\
 &\geq 1/9
 \end{aligned}$$

□

Lemma 1.3. $\| |\psi_0^{t+1}\rangle - |\psi_i^{t+1}\rangle \| \leq \| |\psi_0^t\rangle - |\psi_i^t\rangle \| + \sqrt{q_i^t}$

Proof.

$$\begin{aligned}
 \| |\psi_0^{t+1}\rangle - |\psi_i^{t+1}\rangle \| &= \| U_{t+1}|\psi_0^t\rangle - U_{t+1}O_{\vec{i}}|\psi_i^t\rangle \| && \text{by definition and } O_{\vec{0}} = \text{Id} \\
 &= \| |\psi_0^t\rangle - O_{\vec{i}}|\psi_i^t\rangle \| && \text{unitary preserves norm} \\
 &= \| O_{\vec{i}}(|\psi_0^t\rangle - |\psi_i^t\rangle) + (\text{Id} - O_{\vec{i}})|\psi_0^t\rangle \| \\
 &\leq \| O_{\vec{i}}(|\psi_0^t\rangle - |\psi_i^t\rangle) \| + \| (\text{Id} - O_{\vec{i}})|\psi_0^t\rangle \| && \text{by triangle inequality} \\
 &= \| |\psi_0^t\rangle - |\psi_i^t\rangle \| + \| (\text{Id} - O_{\vec{i}})|\psi_0^t\rangle \|
 \end{aligned}$$

We have $\text{Id} - O_{\vec{i}} = |i\rangle\langle i| \otimes (\text{Id} - X)$ where $X = |1\rangle\langle 0| + |0\rangle\langle 1|$. Hence, $\|(\text{Id} - O_{\vec{i}})|\psi_0^t\rangle\| = \|(|i\rangle\langle i| \otimes (\text{Id} - X))|\psi_0^t\rangle\| \leq 2\|(|i\rangle\langle i| \otimes \text{Id})|\psi_0^t\rangle\| = \sqrt{q_i^t}$, where we used that $\|\text{Id} \otimes (\text{Id} - X)\| \leq 2$. □

Theorem 1.4. $Q(\text{OR}) \geq \sqrt{n}/3$

Proof. $n/3 \leq \sum_{i=1}^n \sum_{t=0}^T \sqrt{q_i^t} \leq \sqrt{nT \sum_{i=1}^n \sum_{t=0}^T q_i^t} = \sqrt{nT} \Rightarrow T \geq \sqrt{n}/3$. □

2 Lecture 2

Proposition 2.1. Fix a quantum algorithm making T queries. Let $p(x) \in [0, 1]$ denote the probability that it outputs 1 on input x . Then $\deg(p) \leq 2T$.

Proof. By induction on T : for all $1 \leq i \leq n$, $b \in \{0, 1\}$, $\langle i, b | \psi_x^T \rangle$ is a polynomial in x of degree $\leq T$.

For $T = 0$, $|\psi_x^0\rangle = U_0|0, 0\rangle$. Hence, $\langle i, b | \psi_x^0 \rangle$ is independent from x .

For $T + 1$,

$$\begin{aligned} \langle i, b | \psi_x^{T+1} \rangle &= \langle i, b | U_{T+1} O_x | \psi_x^T \rangle \\ &= \sum_{j,c} \alpha_{j,c} \langle j, c | O_x | \psi_x^T \rangle \quad \text{where we define } \sum_{j,c} \alpha_{j,c}^\dagger |j, c\rangle = U_{T+1}^\dagger |i, b\rangle \text{ (indep. from } x) \\ &= \sum_{j,c} \alpha_{j,c} ((1 - x_j) \langle j, c | \psi_x^T \rangle + x_j \langle j, c \oplus 1 | \psi_x^T \rangle) \\ &\quad \text{since } O_x |j, c\rangle = |j, c \oplus x_j\rangle = (1 - x_j) |j, c\rangle + x_j |j, c \oplus 1\rangle \end{aligned}$$

The proposition follows since $p(x) = \|(\text{Id} \otimes |1\rangle\langle 1|) |\psi_x^T|\|^2 = \sum_{1 \leq i \leq n} |\langle i, 1 | \psi_x^T \rangle|^2$. \square

Theorem 2.2. $Q(f) = \widetilde{\deg}(f)/2$

Proof. Suppose a quantum algorithm computes f with probability $\geq 2/3$ and makes T queries. Let $p(x)$ denote the probability that it outputs 1 on input x . Then:

1. $\deg(p) \leq 2T$ by Proposition 2.1
2. $p(x) \geq 2/3$ when $f(x) = 1$ and $p(x) \leq 1/3$ when $f(x) = 0$, by success condition

In particular, $|p(x) - f(x)| \leq 1/3$ for all x . Hence, $\widetilde{\deg}(f) \leq \deg(p) \leq 2T$. \square

Lemma 2.3. P_{sym} is a polynomial in k and $\deg(P_{\text{sym}}) \leq \deg(P)$.

Proof. Let $S \subseteq \{1, \dots, n\}$ and consider the monomial $x_S = \prod_{i \in S} x_i$.

$$\mathbb{E}_{x \sim B_k} [x_S] = \begin{cases} 0 & \text{if } k < |S| \\ \frac{\binom{n-|S|}{k-|S|}}{\binom{n}{k}} = \frac{k(k-1) \cdots (k-|S|+1)}{n(n-1) \cdots (n-|S|+1)} & \text{otherwise} \end{cases}$$

This is a polynomial in k of degree $\leq |S|$. \square

Lemma 2.4. $P_{\text{sym}}(0) \in [0, 1/3]$ and $P_{\text{sym}}(k) \in [2/3, 1]$ for $k \geq 1$.

Proof. $P(x) \in [0, 1/3]$ for all $x \in B_0$ hence $P_{\text{sym}}(0) = \mathbb{E}_{x \sim B_0} [P(x)] \in [0, 1/3]$.

Similarly, $P(x) \in [2/3, 1]$ for all $x \in B_k$, $k \geq 1$. \square

Lemma 2.5. $\sum_x \phi(x) \cdot P(x) = 0$, $\forall P, \deg(P) < d \Leftrightarrow \phi$ has no monomial of degree $< d$.

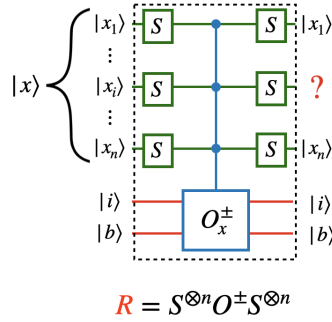
Proof. For any two subsets $S, T \subseteq \{1, \dots, n\}$, $\sum_{x \in \{-1, 1\}^n} x_S x_T = \sum_{x \in \{-1, 1\}^n} x_{S \cap T}^2 x_{T \setminus S} x_{S \setminus T} = \sum_{x \in \{-1, 1\}^n} x_{T \setminus S} x_{S \setminus T} = 2^n \cdot \mathbf{1}_{S=T}$. \square

3 Lecture 3

$$S : \begin{cases} |\emptyset\rangle & \mapsto \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} |y\rangle \\ \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} |y\rangle & \mapsto |\emptyset\rangle \\ \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} \omega^{by} |y\rangle & \mapsto \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} \omega^{by} |y\rangle \quad \text{if } 0 < b < n \end{cases}$$

One can check that:

1. $S^{-1} = S^\dagger$ (unitary) and $S = S^\dagger$ (Hermitian)
2. For all $0 \leq y < n$, $S|y\rangle = |y\rangle + \frac{1}{\sqrt{n}}|\emptyset\rangle - \frac{1}{n} \sum_{0 \leq z < n} |z\rangle$



Lemma 3.1. $R|\dots, x_i = \emptyset, \dots\rangle \otimes |i, b\rangle = \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} \omega^{by} |\dots, x_i = y, \dots\rangle \otimes |i, b\rangle$ when $b \neq 0$.

Proof. We focus on the i -th input register since it is the only register that can change upon applying R .

$$\begin{aligned} |x_i = \emptyset\rangle &\mapsto_S \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} |y\rangle \\ &\mapsto_O \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} \omega^{by} |y\rangle \\ &\mapsto_S \frac{1}{\sqrt{n}} \sum_{0 \leq y < n} \omega^{by} |y\rangle \quad \text{since } b \neq 0 \end{aligned}$$

If $b = 0$ then R acts as the identity: $R|\dots, x_i = \emptyset, \dots\rangle \otimes |i, b\rangle = |\dots, x_i = \emptyset, \dots\rangle \otimes |i, b\rangle$. \square

Lemma 3.2. $R|\dots, x_i = y, \dots\rangle \otimes |i, b\rangle = \omega^{by} |\dots, x_i = y, \dots\rangle \otimes |i, b\rangle + |\text{error}_y\rangle$ when $b \neq 0$

Proof.

$$\begin{aligned} |x_i = y\rangle &\mapsto_S |y\rangle + \frac{1}{\sqrt{n}}|\emptyset\rangle - \frac{1}{n} \sum_{0 \leq z < n} |z\rangle \\ &\mapsto_O \omega^{by} |y\rangle + \frac{1}{\sqrt{n}}|\emptyset\rangle - \frac{1}{n} \sum_{0 \leq z < n} \omega^{bz} |z\rangle \\ &\mapsto_S \omega^{by} |y\rangle + \frac{\omega^{by}}{\sqrt{n}}|\emptyset\rangle - \frac{1}{n} \sum_{0 \leq z < n} \omega^{by} |z\rangle + \frac{1}{n} \sum_{0 \leq z < n} |z\rangle - \frac{1}{n} \sum_{0 \leq z < n} \omega^{bz} |z\rangle \end{aligned}$$

\square

Lemma 3.3. $\Delta_0 = 0$.

Proof. $|\psi_{\text{rec}}^0\rangle = |\emptyset, \dots, \emptyset\rangle \otimes |0, 0\rangle$

\square

Lemma 3.4. $\sqrt{\Delta_{t+1}} \leq \sqrt{\Delta_t} + \sqrt{10/n}$.

Proof.

$$\begin{aligned}
\sqrt{\Delta_{t+1}} &= \|\Pi U_{t+1} R |\psi_{\text{rec}}^t\rangle\| && \text{by } |\psi_{\text{rec}}^{t+1}\rangle = U_{t+1} R |\psi_{\text{rec}}^t\rangle \\
&= \|\Pi R |\psi_{\text{rec}}^t\rangle\| && \text{since } \Pi \text{ and } U_{t+1} \text{ commute} \\
&\leq \|\Pi R \Pi |\psi_{\text{rec}}^t\rangle\| + \|\Pi R (\text{Id} - \Pi) |\psi_{\text{rec}}^t\rangle\| && \text{by triangle inequality} \\
&\leq \|\Pi |\psi_{\text{rec}}^t\rangle\| + \|\Pi R (\text{Id} - \Pi) |\psi_{\text{rec}}^t\rangle\| && \text{by contraction} \\
&= \sqrt{\Delta_t} + \|\Pi R (\text{Id} - \Pi) |\psi_{\text{rec}}^t\rangle\|
\end{aligned}$$

Lemma 3.5. For any state $|\psi\rangle \in \ker(\Pi)$ we have $\|\Pi R |\psi\rangle\| \leq \sqrt{\frac{10}{n}} \| |\psi\rangle \|$

Proof. Let $|\psi\rangle = \sum_{x,i,b} \alpha_{x,i,b} |x\rangle \otimes |i,b\rangle$ (by assumption, $\alpha_{x,i,b} \neq 0 \Rightarrow 1 \notin x$)

We decompose $|\psi\rangle$ into $n+2$ mutually orthogonal states:

- $|\psi_{\text{id}}\rangle = \sum_{x,i,b=0} \alpha_{x,i,b} |x\rangle \otimes |i,b\rangle$
- $|\psi_{\emptyset}\rangle = \sum_{x,i,b:x_i=\emptyset, b \neq 0} \alpha_{x,i,b} |x\rangle \otimes |i,b\rangle$
- $|\psi_y\rangle = \sum_{x,i,b:x_i=y, b \neq 0} \alpha_{x,i,b} |x\rangle \otimes |i,b\rangle$ for all $0 \leq y < n$

We show that:

- $\|\Pi R |\psi_{\text{id}}\rangle\| = 0$ since $R |\psi_{\text{id}}\rangle = |\psi_{\text{id}}\rangle$
- $\|\Pi R |\psi_{\emptyset}\rangle\| = \frac{1}{\sqrt{n}} \| |\psi_{\emptyset}\rangle \|$
- $\|\Pi R |\psi_1\rangle\| = 0$ since $|\psi_1\rangle = 0$
- $\|\Pi R |\psi_y\rangle\| \leq \frac{3}{n} \| |\psi_y\rangle \|$ for all $y \in \{0, 2, \dots, n-1\}$

It will imply by triangle inequality + Cauchy-Schwarz:

$$\|\Pi R |\psi\rangle\| \leq \|\Pi R |\psi_{\emptyset}\rangle\| + \sum_y \|\Pi R |\psi_y\rangle\| \leq \frac{1}{\sqrt{n}} \| |\psi_{\emptyset}\rangle \| + \frac{3}{n} \sum_{y \neq 1} \| |\psi_y\rangle \| \leq \sqrt{\frac{10}{n}} \| |\psi\rangle \|$$

Proof that $\|\Pi R |\psi_{\emptyset}\rangle\| \leq \frac{1}{\sqrt{n}} \| |\psi_{\emptyset}\rangle \|$:

By Lemma 3.1, for any basis state $|x\rangle \otimes |i,b\rangle \in \text{supp}(|\psi_{\emptyset}\rangle)$ with $b \neq 0$, we have

$$\Pi R |x_1, \dots, x_i = \emptyset, \dots, x_n\rangle \otimes |i,b\rangle = \frac{\omega^b}{\sqrt{n}} |x_1, \dots, 1, \dots, x_n\rangle \otimes |i,b\rangle$$

Thus,

$$\Pi R |\psi_{\emptyset}\rangle = \sum_{x,i,b:x_i=\emptyset, b \neq 0} \alpha_{x,i,b} \frac{\omega^b}{\sqrt{n}} |x^{\{i\}}\rangle \otimes |i,b\rangle$$

where $x_i^{\{i\}} = 1 - x_i = 1$ and $x_j^{\{i\}} = x_j$ for $j \neq i$.

$$\text{Finally, } \|\Pi R |\psi_{\emptyset}\rangle\|^2 = \sum_{x,i,b:x_i=\emptyset, b \neq 0} \frac{|\alpha_{x,i,b}|^2}{n} = \frac{1}{n} \| |\psi_{\emptyset}\rangle \|^2.$$

Proof that $\|\Pi R |\psi_y\rangle\| \leq \frac{3}{n} \| |\psi_y\rangle \|$:

By Lemma 3.2,

$$\Pi R |x_1, \dots, x_i = y, \dots, x_n\rangle \otimes |i,b\rangle = \frac{1 - \omega^b - \omega^{by}}{n} |x_1, \dots, 1, \dots, x_n\rangle \otimes |i,b\rangle$$

$$\text{Hence, } \|\Pi R |\psi_y\rangle\|^2 = \sum_{x,i,b:x_i=y, b \neq 0} \frac{|(1 - \omega^b - \omega^{by}) \alpha_{x,i,b}|^2}{n^2} \leq \frac{9}{n^2} \| |\psi_y\rangle \|^2.$$

□

□

4 Lecture 4

Lemma 4.1. $\Delta_0 = \|\Gamma\|$.

Proof. $\Delta_0 = |\langle \psi^0 | \Gamma \otimes \text{Id} | \psi^0 \rangle| = |\langle a | \Gamma | a \rangle| = \|\Gamma\|$ since $|\psi^0\rangle = |a\rangle \otimes |0, 0\rangle$ and a is a principal ev of unit norm. \square

Lemma 4.2. $\Delta_T < 0.95\|\Gamma\|$ if the algorithm succeeds w.p. $\geq 2/3$ after T queries.

Proof. Define $\Pi_{\text{succed}} = \sum_x |x\rangle\langle x| \otimes \text{Id} \otimes |f(x)\rangle\langle f(x)|$

$$\begin{aligned}
\Delta_T &= |\langle \psi^T | \Gamma \otimes \text{Id} | \psi^T \rangle| \\
&= |\langle \psi^T | \Pi_{\text{succed}}(\Gamma \otimes \text{Id})\Pi_{\text{succed}} | \psi^T \rangle + \langle \psi^T | (\text{Id} - \Pi_{\text{succed}})(\Gamma \otimes \text{Id})(\text{Id} - \Pi_{\text{succed}}) | \psi^T \rangle \\
&\quad + \langle \psi^T | \Pi_{\text{succed}}(\Gamma \otimes \text{Id})(\text{Id} - \Pi_{\text{succed}}) | \psi^T \rangle + \langle \psi^T | (\text{Id} - \Pi_{\text{succed}})(\Gamma \otimes \text{Id})\Pi_{\text{succed}} | \psi^T \rangle| \\
&= |\langle \psi^T | \Pi_{\text{succed}}(\Gamma \otimes \text{Id})(\text{Id} - \Pi_{\text{succed}}) | \psi^T \rangle + \langle \psi^T | (\text{Id} - \Pi_{\text{succed}})(\Gamma \otimes \text{Id})\Pi_{\text{succed}} | \psi^T \rangle| \\
&\leq 2\|\Gamma \otimes \text{Id}\| \cdot \|\Pi_{\text{succed}} | \psi^T \rangle\| \cdot \|(\text{Id} - \Pi_{\text{succed}}) | \psi^T \rangle\| \\
&\leq 2\|\Gamma\| \cdot \sqrt{\|\Pi_{\text{succed}} | \psi^T \rangle\|^2 (1 - \|\Pi_{\text{succed}} | \psi^T \rangle\|^2)} \\
&\leq 2\|\Gamma\| \cdot \sqrt{2}/3
\end{aligned}$$

where the third equality is because $\Gamma_{xy} = 0$ when $f(x) \neq f(y)$. \square

Lemma 4.3. $\Delta_{t+1} \geq \Delta_t - 2 \max_{1 \leq i \leq n} \|\Gamma_i\|$.

Proof.

$$\begin{aligned}
\Delta_t - \Delta_{t+1} &\leq |\langle \psi^t | \Gamma \otimes \text{Id} | \psi^t \rangle - \langle \psi^{t+1} | \Gamma \otimes \text{Id} | \psi^{t+1} \rangle| \\
&= |\langle \psi^t | \Gamma \otimes \text{Id} | \psi^t \rangle - \langle \psi^t | O(\Gamma \otimes \text{Id})O | \psi^t \rangle| \quad \text{since } |\psi^{t+1}\rangle = (\text{Id} \otimes U_{t+1})O|\psi^t\rangle \\
&= \left| \sum_{x,y} \Gamma_{x,y} a_x a_y^* \langle \psi_x^t | (\text{Id} - O_x O_y) | \psi_y^t \rangle \right|
\end{aligned}$$

Claim 4.4. $\text{Id} - O_x O_y = \sum_{i: x_i \neq x_j} |i\rangle\langle i| \otimes (\text{Id} - X)$

Proof.

$$\langle i, b | (\text{Id} - O_x O_y) | j, c \rangle = \begin{cases} 0 & \text{if } i \neq j \text{ or } x_i = x_j \\ 1 & \text{if } i = j, x_i \neq x_j, b = c \\ -1 & \text{if } i = j, x_i \neq x_j, b \neq c \end{cases}$$

\square

$$\begin{aligned}
\Delta_t - \Delta_{t+1} &\leq \left| \sum_i \sum_{x,y} (\Gamma_i)_{x,y} a_x a_y^* \langle \psi_x^t | (|i\rangle\langle i| \otimes (X - \text{Id})) | \psi_y^t \rangle \right| \\
&\leq \sum_i |\langle \psi^t | (|i\rangle\langle i| \otimes \sqrt{X})(\Gamma_i \otimes \text{Id})(|i\rangle\langle i| \otimes \sqrt{X}) | \psi^t \rangle| + |\langle \psi^t | (|i\rangle\langle i| \otimes \text{Id})(\Gamma_i \otimes \text{Id})(|i\rangle\langle i| \otimes \text{Id}) | \psi^t \rangle| \\
&\quad \text{by triangle inequality} \\
&\leq \sum_i \|\Gamma_i\| \cdot \|(|i\rangle\langle i| \otimes \sqrt{X}) | \psi^t \rangle\|^2 + \|\Gamma_i\| \cdot \|(|i\rangle\langle i| \otimes \text{Id}) | \psi^t \rangle\|^2 \\
&\leq 2 \max_{1 \leq i \leq n} \|\Gamma_i\| \sum_i \|(|i\rangle\langle i| \otimes \text{Id}) | \psi^t \rangle\|^2 \\
&= 2 \max_{1 \leq i \leq n} \|\Gamma_i\|
\end{aligned}$$

\square