Proof sketches

1 Lecture 1

Lemma 1.1. $\| |\psi_{\vec{0}}^0\rangle - |\psi_{\vec{i}}^0\rangle \| = 0$

Proof. $|\psi_{\vec{0}}^0\rangle = |\psi_{\vec{i}}^0\rangle = U_0|0,0\rangle$ □

Lemma 1.2. $\| |\psi_{\vec{0}}^T\rangle - |\psi_{\vec{i}}^T\rangle \| \geq 1/3$ *if the algorithm succeeds wp* $\geq 2/3$ *after* T *queries*

Proof. Success conditions: $\|(\mathrm{Id} \otimes |0\rangle\langle 0|)|\psi_{\vec{0}}^T\rangle\|^2 \geq 2/3$ and $\|(\mathrm{Id} \otimes |1\rangle\langle 1|)|\psi_{\vec{i}}^T\rangle\|^2 \geq 2/3$

$$\begin{aligned}
\| |\psi_{\vec{0}}^T\rangle - |\psi_{\vec{i}}^T\rangle \|^2 &= 2(1 - \mathrm{Re}(\langle\psi_{\vec{0}}^T|\psi_{\vec{i}}^T\rangle)) \\
&= 2(1 - \mathrm{Re}(\langle\psi_{\vec{0}}^T| \left(\mathrm{Id} \otimes |0\rangle\langle 0|\right) |\psi_{\vec{i}}^T\rangle) - \mathrm{Re}(\langle\psi_{\vec{0}}^T| \left(\mathrm{Id} \otimes |1\rangle\langle 1|\right) |\psi_{\vec{i}}^T\rangle)) \\
&\geq 2(1 - \|(\mathrm{Id} \otimes |0\rangle\langle 0|)\psi_{\vec{0}}^T\| \cdot \|(\mathrm{Id} \otimes |0\rangle\langle 0|)\psi_{\vec{i}}^T\| - \|(\mathrm{Id} \otimes |1\rangle\langle 1|)\psi_{\vec{0}}^T\| \cdot \|(\mathrm{Id} \otimes |1\rangle\langle 1|)\psi_{\vec{i}}^T\|) \\
&\qquad \text{by Cauchy-Schwarz inequality} \\
&\geq 2(1 - 2\sqrt{2}/3) \qquad \text{by success conditions} \\
&\geq 1/9
\end{aligned}$$

□

Lemma 1.3. $\| |\psi_{\vec{0}}^{t+1}\rangle - |\psi_{\vec{i}}^{t+1}\rangle \| \leq \| |\psi_{\vec{0}}^t\rangle - |\psi_{\vec{i}}^t\rangle \| + \sqrt{q_i^t}$

Proof.

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

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

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

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

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 $T+1$,

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

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

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 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, $\widetilde{\deg}(f) \leq \deg(p) \leq 2T$. □

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

Proof. Let $S \subseteq \{1,\ldots,n\}$ 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 $\leq |S|$. □

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

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

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

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

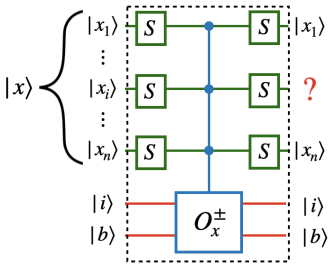
Proof. For any two subsets $S,T \subseteq \{1,\ldots,n\}$, $\sum_{x\in\{-1,1\}^n} x_S x_T = \sum_{x\in\{-1,1\}^n} x_{S\cap T}^2 x_{T\setminus S}x_{S\setminus T} = \sum_{x\in\{-1,1\}^n} x_{T\setminus S}x_{S\setminus T} = 2^n\cdot \mathbf{1}_{S=T}$. □

3 Lecture 3

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

One can check that:

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



$R = S^{\otimes n} O^{\pm} S^{\otimes n}$

Lemma 3.1. $R|\ldots, x_i = \varnothing, \ldots\rangle \otimes |i, b\rangle = \frac{1}{\sqrt{n}} \sum_{0\le y<n} \omega^{by} |\ldots, x_i = y, \ldots\rangle \otimes |i, b\rangle$ *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.

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

If $b = 0$ then R acts as the identity: $R|\ldots, x_i = \varnothing, \ldots\rangle \otimes |i, b\rangle = |\ldots, x_i = \varnothing, \ldots\rangle \otimes |i, b\rangle$. □

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

Proof.

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

□

Lemma 3.3. $\Delta_0 = 0$.

Proof. $|\psi^0_{\text{rec}}\rangle = |\varnothing, \ldots, \varnothing\rangle \otimes |0, 0\rangle$ □

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

Proof.

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

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:

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

We show that:

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

It will imply by triangle inequality + Cauchy-Schwarz:

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

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

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

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

Thus,

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

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

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

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

By Lemma 3.2,

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

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

□

□