Proof sketches

1 Lecture 1

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

Proof. $|\psi^0_{\vec{0}}\rangle = |\psi^0_{\vec{i}}\rangle = U_0|0,0\rangle$ $\square$

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

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

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

$\square$

Lemma 1.3. $\| |\psi^{t+1}_{\vec{0}}\rangle - |\psi^{t+1}_{\vec{i}}\rangle \| \leq \| |\psi^t_{\vec{0}}\rangle - |\psi^t_{\vec{i}}\rangle \| + \sqrt{q^t_i}$

Proof.

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

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, $\|(\mathrm{Id} - O_{\vec{i}})|\psi^t_{\vec{0}}\rangle\| = \|(|i\rangle\langle i| \otimes (\mathrm{Id} - X))|\psi^t_{\vec{0}}\rangle\|| \leq 2\|(|i\rangle\langle i| \otimes \mathrm{Id})|\psi^t_{\vec{0}}\rangle\|| = \sqrt{q^t_i}$, where we used that $\|\mathrm{Id} \otimes (\mathrm{Id} - X)\| \leq 2$. $\square$

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

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

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 $T+1$,

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

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