TD 8

1. Min of a List

1. Grover with Z_{β_i} $\quad \beta_i(x) = \begin{cases} 1 \text{ if } x_i < x \\ 0 \text{ otherwise} \end{cases}$ (easily built for U_{x_i})

Need to know $a = |\beta^{-1}(1)|$

but $a = \underbrace{\text{rank}(x_i)}_{\text{"order in sorted list}} - 1$

So Grover works in $O\left(\sqrt{\frac{N}{a}}\right) = O\left(\sqrt{\frac{N}{r}}\right)$ $\quad \left(\theta = \text{Arcsin}\left(\sqrt{\frac{a}{N}}\right) \simeq \sqrt{\frac{a}{N}}\right)$

Success proba $= \sin^2\left((2k+1)\theta\right) \xrightarrow[N \to +\infty]{} 1$

With $\theta = \text{Arcsin}\left(\sqrt{\frac{a}{N}}\right) \simeq \sqrt{\frac{a}{N}}$

$k = \left\lfloor \frac{\pi}{4\theta} - \frac{1}{2} \right\rfloor \simeq \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{a}} - \frac{1}{2} \right\rfloor$

(implies $2k+1$ close to $\frac{\pi}{2}$)

2. ⓐ $\sum_{i=1}^{N} \underbrace{O\left(\sqrt{\frac{N}{i}}\right)}_{\text{we find min in } N \text{ steps only!}} = O\left(\sqrt{N} \cdot \underbrace{\sum_{i=1}^{N} \frac{1}{\sqrt{i}}}_{= \Theta(\sqrt{N}) \text{ with } \Sigma/\int \text{ comparison}}\right) = O(N)$

ⓑ Call $p(r/k) = \mathbb{P}(r \text{ is picked} \mid k \text{ remaining elements})$ at some point during the algorithm

(BC) $\times$ $p(r/1) = \begin{cases} 0 \text{ if } r > 1 \\ 1 \text{ if } r = 1 \end{cases} = \begin{cases} \frac{1}{r} \text{ if } r \leq k \\ 0 \text{ if } r > k \end{cases}$ Ok

(HR) $\times$ $p(r \mid k+1) = \frac{1}{k+1} + \sum_{i=1}^{k} p\left(r \mid \underbrace{(k+1)-i}_{\text{ith rank ele}}\right) \times \frac{1}{k+1}$ $\quad$ ($r \leq k+1$)

$= \begin{cases} \frac{1}{r} \text{ by HREC for } r \leq (k+1)-i \\ 0 \text{ otherwise} \end{cases}$

$\frac{1}{k+1}$: own choice among solution

$= \frac{1}{k+1}\left[1 + \frac{k+1-r}{r}\right] = \frac{1}{r}$ ∎

© $\mathbb{E}[\#\text{of queries}] = \sum_{n=1}^{N} p(n/N) \times O\left(\sqrt{\frac{N}{n}}\right)$

$p(n/N)$: each n chosen only once

$O\left(\sqrt{\frac{N}{n}}\right)$: complexity with Bob n

$$= O\left(\sqrt{N} \underbrace{\sum_{n=1}^{N} \frac{1}{\sqrt{n}}}_{O(1) \text{ with } \int/\Sigma}\right)$$

$$= O(\sqrt{N}) \quad \blacksquare$$

(d) Markov: $\mathbb{P}(\#\text{queries} \geq t\sqrt{N}) \leq \frac{1}{t}$, take $t = 3$

success $\geq \frac{2}{3}$ fail $\leq \frac{1}{3}$

(when alg stop, it is correct)

---

2. QMA

1. $\times$ 3SAT $\in$ QMA $\Rightarrow$ NP $\subseteq$ QMA
   $\times$ On classical computation, $|\psi\rangle$ witness of NP, will succeed up 1 el 0 for correctness and soundness

2. Ignore simply $|\psi\rangle$.

3. Take m copies of circuit; and majority vote
   Witness $|\psi\rangle^{\otimes m}$
   Majority vote with majority threshold $= c(m) - \varepsilon$, $\varepsilon = \frac{1}{c\,\text{poly}(m)}$
   So $\mathbb{P}(\text{output} = 1 \mid x \in L_{YES}) = \mathbb{P}(\text{Bin}(c(m), m) \geq (c(m) - \varepsilon)m)$

$$= \mathbb{P}\left(\frac{\mathrm{Bin}(c(n), m)}{m} - c(n) \geq -\varepsilon \right)$$

$$\geq 1 - e^{-2m\varepsilon^2} \text{ by Chernoff bound.}$$

Furthermore, $\forall |\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_m\rangle$ ⚠ ISSUE ⚠

we have a boundedness $\leq s(n)$ on each tensor.

So with the same majority vote, we would get that:

$$\mathbb{P}(\text{output} = 0 \mid x \in L_{NO}) = \mathbb{P}\left(\mathrm{Bin}(s(n), m) < \underbrace{(c(n) - \varepsilon)}_{(s(n) + \varepsilon)} m\right)$$

$$= \mathbb{P}\left(\frac{\mathrm{Bin}(s(n), m)}{m} - s(n) < \varepsilon \right) \geq 1 - e^{-2m\varepsilon^2}$$

So $\mathbb{P}(\text{output} = 1 \mid x \in L_{NO}) \leq e^{-2m\varepsilon^2}$

Take $\boxed{m = \frac{\left(2\,\mathrm{poly}\left(\frac{1}{\varepsilon}\right)(n)\right)^2 \times \ln(3)}{2}}$ gives $e^{-2m\varepsilon^2} = e^{-\ln(3)} = \frac{1}{3}$ ■

ISSUE: Not necessarily a product state in SOUND NESS !

↳ Can be solved but not with our tools yet.

4. (a) × Sample j uniformly $\Leftrightarrow$ ancilla $|0^{\log n}\rangle$ — $H^{\otimes \log n}$ and controlled gates

× $V_j^\dagger$: only qubits where H_j act matter, so we can leave the rest of the basis unchanged : constant size ! (so poly size)

× Instead of measure all the qubit we do:

$|0\rangle$ — V_Φ — $|0 \otimes z_1 v \dots v z_{m-m_i}\rangle$ and measure 1 st qubit.

$\notin [m_j]$

$\in [m_j]$

(b) $\mathbb{P}\left(\begin{matrix}\text{getting } i \\ j \text{ chosen}\end{matrix}\right) = |\langle i| V_j^\dagger |\eta\rangle|^2$

$= |(V_j|i\rangle)^\dagger |\eta\rangle|^2$

$= |\langle b_i^j|\eta\rangle|^2 = \langle\eta| b_i^j \times b_i^j |\eta\rangle$

$\mathbb{P}(\text{output}=1) = 1 - \mathbb{P}(\text{output}=0) = 1 - \sum_{i\in[m_j]} \langle\eta| b_i^j \times b_i^j |\eta\rangle = 1 - \langle\eta| H_j |\eta\rangle$

So $\mathbb{P}(\text{output}=1) = \sum_{j=1}^{n} \underbrace{\mathbb{P}(j \text{ chosen})}_{=\frac{1}{n}} \mathbb{P}(\text{output}=1 \mid j \text{ chosen})$

$= \frac{1}{n} \sum_{j=1}^{n} (1 - \langle\eta| H_j |\eta\rangle)$

Thus $\boxed{\mathbb{P}(\text{output}=1) = 1 - \frac{\langle\eta| H |\eta\rangle}{n}}$

(c) On $|\eta\rangle$, we have $H|\eta\rangle = \lambda_{min}|\eta\rangle$

Completeness $\Rightarrow \langle\eta| H |\eta\rangle = \lambda_{min}$

So $\mathbb{P}(\text{output}=1) = 1 - \frac{\lambda_{min}}{n} \geq \boxed{1 - \frac{a}{n}} = c$

(d) For the soundness, we have that $\boxed{\forall |\psi\rangle,\ \langle\psi| H |\psi\rangle \geq \lambda_{min}}$

$\Rightarrow \mathbb{P}(\text{output}=1) \leq 1 - \frac{\lambda_{min}}{n} \leq \boxed{1 - \frac{b}{n}} = s$

(e) But $c - s = \frac{b-a}{n} = \frac{1}{n\,\text{poly}(n)}$: we are in QMA by Q3