lec 4 last part May 18, 2010

Note Title 18/05/2010

Proof of the statement:

Given $\frac{1}{5} > \varepsilon > 0$, $\exists$ n large enough

s.t. $\exists$ $K = (\log n)^3$ bases satisfying

$(*)$ $\forall |\psi\rangle \in \mathbb{C}^n$ $\frac{1}{K}\sum_{t=1}^{K} H_t(|\psi\rangle) > \left[(1-\varepsilon)\log n\right] - 3$

Ideas: (0) Give an existential proof – if we pick k bases at random, iid, then $(*)$ true wp $\gneq 0$

ie we show

$(\bar{*})$ $\exists |\psi\rangle \in \mathbb{C}^n$ $\frac{1}{K}\sum_{t=1}^{K} H_t(|\psi\rangle) \leq \left[(1-\varepsilon)\log n\right] - 3$

holds wp $\lneq 1$ (over the choice of the k bases).

Idea (1) Discretization of $\mathbb{C}^n$ + continuity of $H_t(|\alpha\rangle)$

Instead of checking all $|\psi\rangle \in \mathbb{C}^n$

consider $|\phi\rangle \in S$ a finite subset in $\mathbb{C}^n$

s.t. $\forall |\psi\rangle \in \mathbb{C}^n$

$\exists |\phi\rangle \in S$ with $\left\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \right\|_{Tr} < \varepsilon_0 = \frac{\varepsilon}{2}$

S is called an "ε_0-net" for $\mathbb{C}^n$. We can approx any state in $\mathbb{C}^n$ by one in S.

Can find $|S| \leq \left(\frac{5}{\varepsilon_0}\right)^{2n} = \left(\frac{10}{\varepsilon}\right)^{2n}$ ← exp in dim; gentler dependence on accuracy required

Note $|H_t(|\psi\rangle) - H_t(|\phi\rangle)|$

$\leq \left[\frac{\varepsilon}{2}\log n\right] + 1$ by Fannes Ineq (covered later) & mono of Tr dist under Q ops

$(\bar{*})$ $\exists |\psi\rangle \in \mathbb{C}^n$ $\frac{1}{K}\sum_{t=1}^{K} H_t(|\psi\rangle) \leq \left[(1-\varepsilon)\log n\right] - 3$

$(\bar{*}')$ $\exists |\phi\rangle \in S$ $\frac{1}{K}\sum_{t=1}^{K} H_t(|\phi\rangle) \leq \left[\left(1-\frac{\varepsilon}{2}\right)\log n\right] - 2$

$(\bar{*}) \Rightarrow (\bar{*}')$ $\therefore$ NOT $(\bar{*}') \Rightarrow$ NOT $(\bar{*})$

$\therefore$ Suffices to show $(\bar{*}')$ happens wp $\lneq 1$.

Idea (2): Union bdd.

For $E_1, \ldots, E_r$ r events,

$\Pr(E_1 \text{ or } E_2 \cdots \text{ or } E_r) \leq \sum_{i=1}^{r} \Pr(E_i) \leq r \max_i \Pr(E_i)$

$\therefore \Pr_{k \text{ bases}}\left[\exists |\phi\rangle \in S \ \frac{1}{K}\sum_{t=1}^{K} H_t(|\phi\rangle) \leq \left(1-\frac{\varepsilon}{2}\right)\log n - 2\right]$

$\leq |S| \underbrace{\Pr_{k \text{ bases}}\left[\frac{1}{K}\sum_{t=1}^{K} H_t(|\phi\rangle) \leq \left(1-\frac{\varepsilon}{2}\right)\log n - 2\right]}_{\text{indep of } |\phi\rangle \ \because \text{ bases are random}}$

saves a max over $|\phi\rangle$.

Same as pick $|\phi\rangle$ at random & meas in comp basis.

Idea (3) Use meas conc to bdd the prob of exceptionally low $H(|\phi\rangle)$

comp basis

By Levy's Lemma:

use $\eta = 2 - \Delta$

const $\simeq 10^{-2}$

$\Pr_{|\phi\rangle}\left(\left|H(|\phi\rangle) - \underbrace{\mathbb{E}\, H(|\phi\rangle)}_{\log n - \Delta}\right| > \eta\right) \leq 4 \cdot 2^{-\frac{C n \eta^2}{(\log n)^2}}$

$\log n - \Delta$, Lipschitz const^2 of fcn $|\phi\rangle \to H(|\phi\rangle)$

$\Delta \in [\frac{1}{2}, 1]$

Generically very chaotic outcome

$\therefore \Pr_{|\phi\rangle}\left(H(|\phi\rangle) < \log n - 2\right) \leq 4 \cdot 2^{-(C(2-\Delta)^2)\frac{n}{(\log n)^2}}$

Idea (4): Chernoff bdd over the average of K bases.

$\Pr_{K \text{ iid draws of } |\phi\rangle}\left[\frac{1}{K}\sum_{t=1}^{K} H(|\phi_t\rangle) < \left(1-\frac{\varepsilon}{2}\right)(\log d - 2)\right] \leq 2^{-\frac{K\varepsilon}{2}\frac{n\, C(2-\Delta)^2}{(\log n)^2}}$

Intuition: for the ave < unlikely low entropy a const fraction of the outcomes has to be that low.

By indep, $\Pr(\text{ave low}) \sim \Pr(\text{each low})^{O(K)}$

Finally, want RHS $< \frac{1}{|S|} = \left(\frac{\varepsilon}{10}\right)^{2n} = 2^{-(\ln\frac{\varepsilon}{10})2n}$

$\therefore K = (\log n)^3$ will do.