LECTURE 23 (April 15^{th})

TODAY Area Laws wrapup
Complexity of quantum states & Transformations

RECAP Area Laws in 1-D

Let $H = \sum_{i=1}^{n-1} H_i$ where H_i acts on qudits i & $i+1$

We will assume that

① ground state $|\psi\rangle$ of H is unique

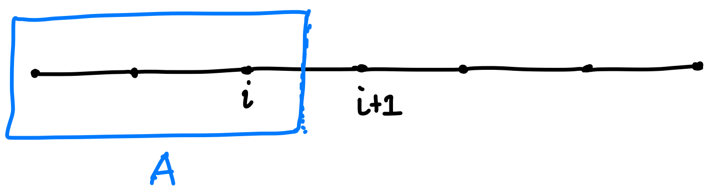
② each H_i is a projector, i.e., $H_i^2 = H_i$

③ $\lambda_{min}(H) = 0$

$\Big\}$ not necessary

④ spectral gap: the second lowest eigenvalue is $\Omega(1)$

$\boxed{\text{Theorem}}$ For any cut $(i, i+1)$, the entanglement entropy of $|\psi\rangle$ is $O(1)$.



Commuting Hamiltonians $\quad H_iH_j = H_jH_i \quad \forall i \neq j$

Claim $\quad P = (\mathbb{1} - H_1) \cdots\cdots (\mathbb{1} - H_{n-1}) = |\psi\rangle\langle\psi|$
is a projector with schmidt rank at most d^2 and it projects on to the ground state $|\psi\rangle$

Then, consider the state $\dfrac{P|\phi\rangle}{\|P|\phi\rangle\|} = |\psi\rangle$ since $P = |\psi\rangle\langle\psi|$

Since $SR(P) \le d$, $SR(|\psi\rangle) \le d \cdot SR(|\phi\rangle) = d$

Thus, Entanglement entropy across any cut is $\log d^2 = O(1)$

Non-commuting Hamiltonians $\quad$ In this case $P = (\mathbb{1} - H_1)(\mathbb{1} - H_2) \cdots\cdots (\mathbb{1} - H_{n-1})$ is not a projector [Why?], so the above proof does not work

This requires some new ideas, but overall strategy remains similar

The first new idea we will need is the notion of an approximate ground space projector (AGSP)

This will be an operator P s.t.

(i) $P|\psi\rangle = |\psi\rangle$ where $|\psi\rangle$ is the unique ground state
i.e. Ground state is preserved

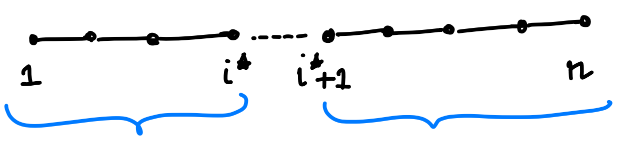
(ii) $\| P|\psi^{\perp}\rangle\|^2 \leq \delta \| |\psi^{\perp}\rangle \|^2$ where $|\psi^{\perp}\rangle$ is orthogonal to $|\psi\rangle$
i.e. Orthogonal states shrink

It turns out that if we have a sufficiently good AGSP we can carry out the previous proof strategy

$\boxed{\text{Lemma}}$ If $\exists$ an AGSP P with schmidt rank $SR(P) \leq r$ and $\delta \leq \frac{1}{2r}$ then the entanglement entropy of ground state $|\psi\rangle$ across any cut (i^*, i^*+1) is $O(\log r)$.

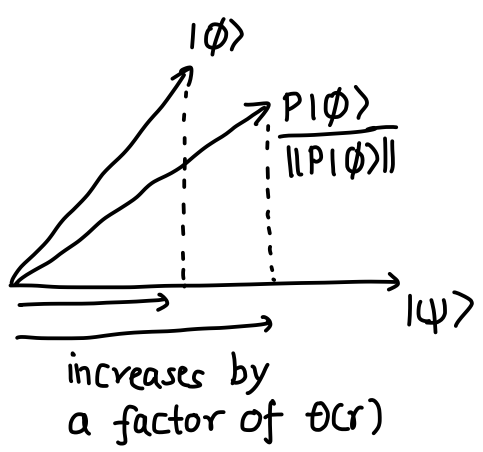
We will talk about how to construct a good AGSP later but the proof of this lemma goes in the following way

Claim 1. Existence of AGSP as stated implies that there is a product state $|\phi\rangle$ that has a large overlap with the ground state, i.e. $|\langle\phi|\psi\rangle| \geq \frac{1}{\sqrt{2r}}$



$|\phi\rangle = |\phi_L\rangle \otimes |\phi_R\rangle \Rightarrow$ No entanglement entropy across cut

Claim 2. Applying the AGSP to this state shrinks the part orthogonal to $|\psi\rangle$
Thus, the normalized state $\frac{P|\phi\rangle}{\|P|\phi\rangle\|}$ has more overlap with $|\psi\rangle$



If we keep repeating it, we will get closer to the ground state and the entanglement entropy does not increase too much in each step

<u>Proof of Claim 1</u>

Consider the product state $|\phi\rangle$ that has the largest overlap with $|\psi\rangle$ and let $|\langle\phi|\psi\rangle| = \mu$

Then, $|\phi\rangle = \mu|\psi\rangle + \sqrt{1-\mu^2}\,|\psi^\perp\rangle$

Applying P, $P|\phi\rangle = \mu|\psi\rangle + \delta|\tilde{\psi}^\perp\rangle$ where $\delta^2 \leq \frac{1}{2r}$

Moreover, schmidt decomposition of the unnormalized state $P|\phi\rangle$ has at most r terms, $P|\phi\rangle = \sum_{i=1}^{r} \sigma_i \underbrace{|u_i\rangle \otimes |v_i\rangle}_{\text{orthonormal}}$

$$\sum_{i=1}^{r} \sigma_i^2 = \| P|\phi\rangle \|^2 \leq \mu^2 + \delta^2$$

Also, $\mu = |\langle\psi|P|\phi\rangle| \leq \sum_{i=1}^{r} \underbrace{\sigma_i}_{\geq 0} \underbrace{|\langle\psi|\,|u_i\rangle\otimes|v_i\rangle|}_{\leq \mu}$

$$\Rightarrow \sum_{i=1}^{r} \sigma_i \geq 1 \Rightarrow \sum_{i=1}^{r} \sigma_i^2 \geq \frac{1}{r} \quad \text{by Cauchy-schwarz}$$

Thus, $\mu^2 + \delta^2 \geq \frac{1}{r} \Rightarrow \mu \geq \frac{1}{\sqrt{2r}}$

<u>Proof of claim 2</u>

We start with a product state $|\phi\rangle$ with overlap $\mu \geq 1/\sqrt{2r}$

Then, overlap of $|\phi_1\rangle = \frac{P|\phi\rangle}{\|P|\phi\rangle\|} \geq \frac{\mu}{\sqrt{\mu^2+\delta^2}} \geq \frac{1/\sqrt{2r}}{\sqrt{\frac{1}{2r}+\frac{1}{2r}}} \geq \frac{1}{\sqrt{2}}$

and schmidt rank of $|\phi_1\rangle \leq r$

If we iterate, overlap keeps increasing and schmidt rank also keeps increasing in each iteration $(r \to r^2 \to r^3 \to \cdots)$

However, with a careful analysis, one can show that the entanglement entropy at the end behaves like the entropy of the following distribution over $[d^n]$

want r to not depend on n

$1/2$ probability mass over $\{1, \ldots, r\}$

$1/2 + 1/2^2$ probability mass over $\{1, \ldots, r^2\}$ and so on

$$\text{Entropy of this distribution} \leq \frac{1}{2}\log r + \frac{1}{2^2}\log r^2 + \cdots$$

$$\leq \sum_{j=1}^{\infty} \frac{j}{2^j} \log r = O(\log r)$$

To complete the proof of Area law, we need to construct an AGSP

$\boxed{\text{Lemma}}$ $\exists$ a good AGSP with schmidt rank $\leq 2^{O(\log^3 d)}$

$\Rightarrow$ This together with the last lemma implies that the entanglement entropy across any cut is at most

$$O(\log^3 d) = O_d(1)$$

Remark: *If one can improve the schmidt rank to poly(d) this would also imply an area law in higher dimensions.*

We will not prove this lemma here since it is fairly involved but we illustrate the main idea

The first thing one can try is

$$P = (\mathbb{1} - H_1)(\mathbb{1} - H_2) \cdots\cdots (\mathbb{1} - H_{n-1}) \quad \text{as before}$$

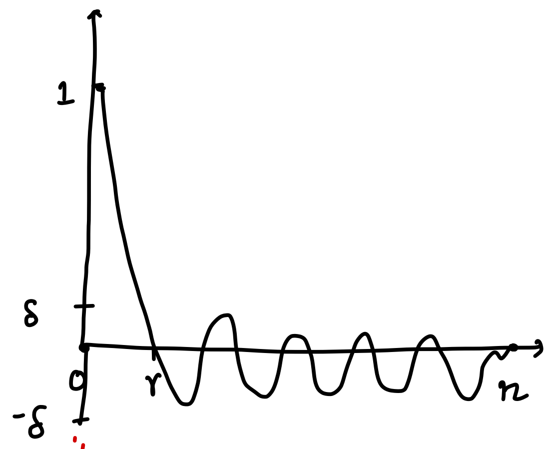
This has schmidt rank $\sim d^2$ but the shrinking factor is only constant where as we would want $1/2d^2$

To get around this one can use a different polynomial in H_i's

Let's restrict to applying a univariate polynomial $q(H)$ where $H = \sum H_i$ since this preserves the eigenvectors of H

- if $|\phi\rangle$ is an eigenvector of H with eigenvalue λ, then $|\phi\rangle$ is also an eigenvector of $q(H)$ with eigenvalue $q(\lambda)$
- eigenvalues of H are $0, \gamma = \Omega(1), \ldots\ldots$
- We want $q(H)$ to be our AGSP, so $q(H')$ should map $|\psi\rangle$ to $|\psi\rangle$ which implies that $q(\lambda) = 1$ for $\lambda = 0$
- Similarly, all the orthogonal eigenvectors should shrink by a factor of δ so, $|q(\lambda)| \leq \delta \quad \forall \lambda \in [\gamma, n]$

Thus, we want a polynomial q that looks like



The degree of the polynomial and the size of the interval determine the schmidt rank, so we want the smallest degree polynomial that looks like this. These are called Chebyshev polynomials.

Look at the linked references if you are interested in more details on how to construct AGSPs using Chebyshev polynomials

Complexity of quantum states and transformations

So, far we have mostly looked at problems where the inputs and outputs are classical

Now, we will talk about the complexity of problems with quantum inputs or outputs

- State and Unitary synthesis
  - What is the complexity of synthesizing states and unitaries?
  - How much of the complexity of these tasks is classical, versus that due to quantum aspects?

- Quantum pseudorandomness and applications
  - How to construct states or unitaries that look random?
  - What can we do with them?

State and Unitary Synthesis

Given a state $|\psi\rangle$, its complexity $C_\varepsilon(|\psi\rangle)$ is the minimum size of a quantum circuit that computes $|\psi\rangle$ upto error ε.

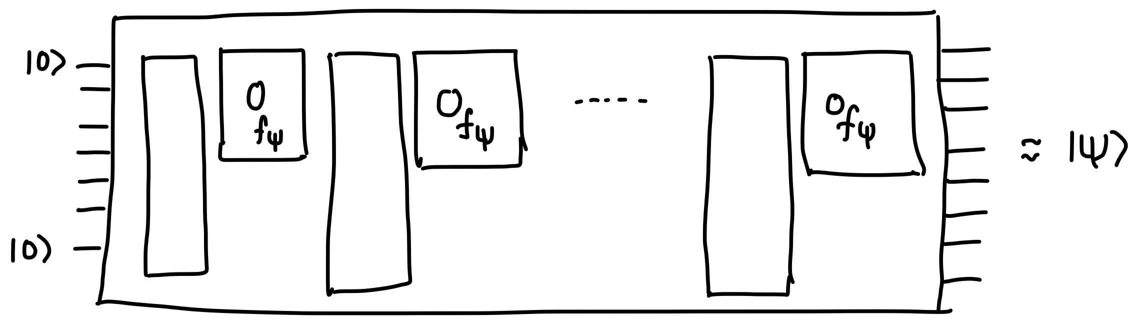
A simple counting argument shows that for most n-qubit states $|\psi\rangle$

$$C_\varepsilon(|\psi\rangle) = 2^{\Omega(n)}$$

The same is true for classical boolean functions: most boolean functions on n-bits need circuits of size $2^{\Omega(n)}$

This motivates the question: can the complexity of synthesizing a quantum state be reduced to the complexity of computing a boolean function

<u>State synthesis problem</u> Is there a quantum query algorithm, a polynomial $p(n)$ and an encoding schme that maps n-qubit states $|\psi\rangle$ to a function $f_\psi : \{0,1\}^{p(n)} \to \{0,1\}$ s.t. A makes poly(n) queries to f_ψ and outputs a good approximation to $|\psi\rangle$?



where $O_{f_\psi} |x\rangle|b\rangle \to |x\rangle|b \oplus f_\psi(x)\rangle$ for $x \in \{0,1\}^{p(n)}$

If the answer is yes, then in this sense state synthesis is no harder than computing an appropriate boolean function

NEXT TIME State and Unitary Synthesis