LECTURE 19 (March 26^{th})

TODAY QMA(2) wrapup
Complexity of Ground States of Local Hamiltonians

Detecting Mixed-state Entanglement and Complexity of QMA(2)

QMA(2) is connected to one of the most fundamental problems in quantum information:

Given a classical description of a quantum state, is it entangled or not?

There are two relevant formulations here

① Pure state entanglement   If $|\psi\rangle = |\varphi\rangle \otimes |\theta\rangle$ or not?

One can solve this by taking the partial trace of the first system and checking if we get a pure state or not

Takes poly(d) time classically if $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$

② Mixed state entanglement   Given a density matrix ρ on two registers A and B, each of dimension d, determine if ρ is separable

ρ is separable if

$$\rho = \sum_i p_i \, \sigma_i \otimes \tau_i$$ for σ_i, τ_i density matrices in $\mathbb{C}^d \times \mathbb{C}^d$ and $\{p_i\}$ probability distribution

Separable states don't have entanglement but might have classical correlations
E.g. two coin tosses that are perfectly correlated similar to the EPR pair

How can we determine if ρ is separable?

In fact, this problem is NP-complete in the worst case (shown by Gurvits)

What about approximations? i.e. Given ε, is ρ separable or ε-far (say in trace distance) from any separable state, promised that one is the case?

Is there an algorithm for this task?

We don't know: some conjecture that there is a $2^{O(\log^2 d)}$ time algorithm while others conjecture that exponential in d time is needed
(Some quasi-polynomial algorithms are known for approximation in other norms)

General belief is that detecting pure state entanglement is easy, but it is hard for mixed states

How is this related to QMA(2)?

Huge complexity class

Currently, we know QMA $\subseteq$ QMA(2) $\subseteq$ NEXP

We also know that QMA $\subseteq$ EXP since one has to compute eigenvalues of $2^m \times 2^m$ matrix which can be done in poly(2^m) time where $m = \text{poly}(n)$ is the number of qubits

Recall that $\lambda_{max}(M) = \max_{|\psi\rangle} \langle\psi|M|\psi\rangle$

If there was a $2^{O(\log^2 d)} = 2^{O(m^2)}$ algorithm to decide if a state is separable or not, then one can solve the following problem in $2^{poly(m)}$ time

$$\text{Find} \quad \max_{|\psi\rangle\otimes|\theta\rangle} \langle\psi|\otimes\langle\theta| \; M \; |\theta\rangle\otimes|\psi\rangle$$

where we optimize only over separable states

This would imply that QMA(2) $\subseteq$ EXP

It turns out that the separable states problem is connected to many fundamental questions in classical computer science such as the Unique Games Conjecture, optimizing over tensors, and so on

So, is QMA(2) = QMA or QMA(2) = NEXP or something in between?

Very active developments in the last couple of years with mixed evidence?

$\boxed{1}$ Is QMA(2) = QMA?

One natural approach for QMA verifier to simulate a QMA(2) protocol is to come up with a disentangler

Given any arbitrary QMA proof,
map it to an (approximately) separable state

If such an object (with suitable parameters) existed, then QMA(2) = QMA

Consider the following disentangler :

① take a state on registers $R_0, R_1, \dots R_N$
② choose a register $i \in [N]$ at random
③ output the state on R_0 and R_i

Quantum DeFinetti Theorems imply that this is close to a separable state if $N = 2^n$

Here input dimension is exponentially larger than the output dimension

If one could show that such a disentangler exists with input dimension being quasi-polynomial in the output dimension, i.e.

$$\text{input-dimension} = 2^{\text{polylog}(\text{output-dimension})}$$

and it can efficiently computed by a quantum algorithm, then $QMA(2) = QMA$

No Disentangler Conjecture of Watrous says that input-dimension must always be larger exponentially larger even for constant approximation

2 <u>Is $QMA(2) = NEXP$? or $QMA(2)_{\log} = NP$?</u>

Recent work of Jeronimo and Wu showed that if one restricts the QMA(2) witnesses to only have positive amplitudes, then the resulting class

$$QMA^+(2) = NEXP$$

Some followup work by Bassirian, Fefferman and Marwaha showed that the same is true for QMA

$$QMA^+ = NEXP$$

Many interesting questions remain open :

- is there an oracle separation between QMA and QMA(2) ?
- if the proofs have limited entanglement, what happens ?

I hope you can answer some of them

PART III Complexity of Ground States of Local Hamiltonians

Motivating question for the next few lectures

"Which local Hamiltonians have ground states (or low-energy states) that are simple?"

What do we mean by simple?

We want to capture states that have a simple entanglement structure e.g. tensor product of 1 or 2-qubit states

One of the most efficient ways we know is via tensor networks that we will introduce in the next lecture

For now, let's start with a more natural notion

Given an n-qubit state $|\psi\rangle$,

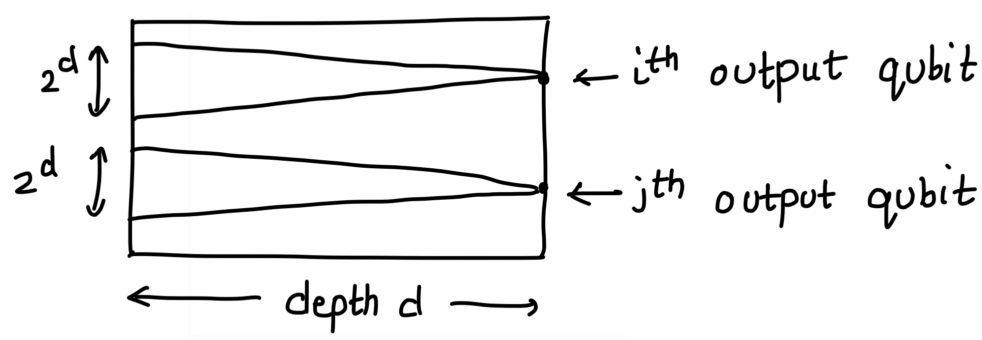
may be hard to find

depth$(|\psi\rangle)$ = minimum depth of a circuit C such that $C|0\rangle^{\otimes n} \approx |\psi\rangle$

Examples (1) Product state $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$ has depth $O(1)$ No entanglement

(2) CAT state $\frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$ has depth $\Omega(\log n)$ Some entanglement

Sketch



If depth was d, the i^{th} output qubit only depends on 2^d input qubits called the "light cone" and same for j^{th} qubit

If $d < \frac{\log n}{1000}$, then the light cones are disjoint

This will imply that measuring i^{th} qubit does not affect the j^{th} qubit which is not true for the CAT state

(3) Random quantum state has depth $2^{\Omega(n)}$ Maximal amount of entanglement

One can consider states with superpoly(n) depth as complicated phases of matter with complex entanglement

Now a fascinating answer to our question from before would be

"all physically relevant Hamiltonians"

because for states with thousands of particles, if their complexity was exponential the universe wouldn't be old enough to prepare them by physical processes that are simulatable by a quantum computer

This would mean that all physically-relevant Hamiltonians have low-energy states that are simple

This would be a huge breakthrough in many-body physics and we will see some results motivated by this question in the next few lectures

- Quantum PCP Conjecture
- Tensor Networks
- Area Laws

Classical PCP Theorem

Recall the Local Hamiltonian Problem

Given $H = \frac{1}{m}\sum_{i=1}^{m} H_i$ where H_i are k-local and $0 \preccurlyeq H_i \preccurlyeq I$

Determine if $\lambda_{min}(H) \leq a$ or $\lambda_{min}(H) \geq a + 1/poly(n)$ where $n = \#$ qubits

This tells us that estimating ground energy of local Hamiltonian upto $\pm \frac{1}{poly(n)}$ precision is a QMA-hard problem

What happens if we want a coarser approximation say with constant error ?

We don't have an answer to this problem yet, but we have an amazing answer to the classical analog of this question

To state what it says, let $\varphi = (x_{i_1} \vee x_{i_2} \vee x_{i_3}) \wedge (\cdots)$ be a 3SAT formula
We saw that one can define a diagonal Hamiltonian

$$H = \frac{1}{m}\sum_{i=1}^{m} H_i$$

such that for any basis state $|x\rangle$ where $x \in \{0,1\}^n$,

$$\langle x|H_i|x\rangle = \begin{cases} 0 & \text{if } x \text{ satisfies clause } i \\ 1 & \text{otherwise} \end{cases}$$

This means that $\lambda_{min}(H) = 0$ if φ is a satisfiable formula
and $\lambda_{min}(H) \geq \frac{1}{m}$ if φ is unsatisfiable

Moreover, $\lambda_{min}(H) = 1 - \text{MAXSAT}(\varphi)$

where $\text{MAXSAT}(\varphi)$ = maximum fraction of clauses satisfiable by any given assignment

From this, it is obvious that determining ground energy of this 3SAT Hamiltonian with $\frac{1}{2m}$ precision is NP-complete :

decide if $\lambda_{min}(H) = 0$ or $\lambda_{min}(H) \geq \frac{1}{2m}$

Equivalently: $\text{MAXSAT}(\varphi) = 1$ or $\text{MAXSAT}(\varphi) \leq 1 - \frac{1}{2m}$

The PCP Theorem gives a robust version of this statement

PCP Theorem $\forall \varepsilon > 0$ and any 3SAT instance φ,
deciding if $\text{MAXSAT}(\varphi) = 1$ or $\text{MAXSAT}(\varphi) \leq 7/8 + \varepsilon$ is NP-hard

A uniformly random assignment satisfies $7/8^{th}$ fraction of clauses on average so deciding if

$$\text{MAXSAT}(\varphi) = 1 \quad \text{or} \quad \text{MAXSAT}(\varphi) \leq 7/8 \quad \text{is trivial}$$

So, the problem goes from NP-hard to trivial and even approximating it to a factor $7/8$ is hard

As the name suggests, the proof relies on the idea of a probabilistically checkable proof

<u>Def</u> Let $L \in NP$. We say L has a probabilistically checkable proof if $\exists$ randomized poly-time verifier that queries $O(1)$ bits of the proof s.t.

(1) $x \in L \implies \exists$ proof π s.t. $\mathbb{P}[V \text{ accepts } (x,\pi)] \geq 2/3$
(2) $x \notin L \implies \forall$ proofs π $\quad \mathbb{P}[V \text{ accepts } (x,\pi)] \leq 1/3$

A PCP is a proof that can be spot-checked. By reading a constant number of bits we can verify its correctness with confidence

The proof-checking formulation of the PCP theorem is then the statement

"every language $L \in NP$ has a probabilistically checkable proof"

This is one of the major breakthroughs in complexity and the proof is remarkable

We will not be able to cover it here but the basic idea is the following

For a languge like 3SAT, the PCP proof consists of encoding a satisfying assignment using a carefully designed error-correcting code that enables easy verification

To translate this statement back to the MAXSAT approximation, one must convert the checks performed by a PCP verifier into a 3SAT formula, using similar ideas to the Cook-Levin theorem which encodes the computational history of the verifier into a 3SAT formula

Quantum PCP Conjecture

The quantum PCP conjecture is similar where replace NP with QMA and 3SAT with K-Local Hamiltonian problem

Quantum PCP Conjecture

$\exists$ a family of k-Local Hamiltonians, one for each qubit size n

$$H = \frac{1}{m}\sum_{i=1}^{m} H_i \quad \text{where } m = \text{poly}(n)$$

such that deciding if $\lambda_{\min}(H) \leq a$ or $\lambda_{\min}(H) \geq a+\varepsilon$ is QMA-hard for universal constants $k, a, \varepsilon > 0$.

Note $b - a = \varepsilon > 0$ is a constant here as opposed to inverse polynomial