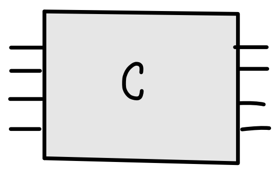
LECTURE 13 (February 28^{th})

TODAY Random Circuit Sampling (contd)
Quantum Proofs and QMA

RECAP The task we looked in the last lecture was random circuit sampling



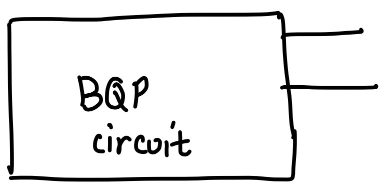
quantum circuit

Sample from output distribution of a simple quantum circuit

The goal was to demonstrate practical quantum advantage, i.e. there is no classical algorithm that can even sample from a distribution that is close to the above (e.g. in TV distance)

To do this, we first considered the case where we rule out exact samplers

For this we introduced the notion of postselection



postselection bits $P \in \{0,1\}^{poly(n)}$
output bit A

and similarly for BPP algorithms

$$\mathbb{P}[\, A \text{ is correct} \mid P = 0 \cdots 0\,] \geq \frac{2}{3}$$

Postselection is not physical! We can take as much time as we want to postselect. For instance, we run the BQP (or BPP circuit) exponentially or doubly exponential times to estimate all probabilities with tiny error and then we can postselect

We saw that postBQP = PP, so BQP with postselection can solve very hard problems and even simple quantum circuit classes with postselection become as powerful

On the other hand, postBPP $\neq$ PP unless PH collapses

This means that even the existence of an exact classical sampler that works for the worst-case quantum circuit would imply that PH collapses

Same argument also works if the classical sampler gave a $(1+\varepsilon)$-multiplicative approximation.

What about a classical sampler that is ε-close in TV-distance?

$$\frac{1}{2} \sum_{y \in \{0,1\}^n} |p_C(y) - q_C(y)| \leq \varepsilon$$

$$\Rightarrow \mathbb{E}_y |p_C(y) - q_C(y)| \le \frac{2\varepsilon}{2^n}$$

$\Rightarrow$ For 99% of y's,

$$|p_C(y) - q_C(y)| \le \frac{200\varepsilon}{2^n}$$

Using Stockmeyer's algorithm, we saw that such a classical sampler can be used to get a BPP^{NP} algorithm that outputs an estimate

$$\hat{p}_y \in \left(1 \pm \frac{1}{poly(n)}\right) q_C(y) + O\left(\frac{\varepsilon}{2^n}\right) \text{ approximation for 99\% of } y\text{'s}$$

If we also pick a circuit C at random and suppose that

with prob. 0.8, C is anticoncentrated, i.e. most y's satisfy $q_C(y) \geq \frac{1}{100 \cdot 2^n}$

then the above implies that

w.p. 0.75 over (C, y) we can get a multiplicative $1 \pm \frac{1}{poly(n)}$ approximation

to the output probabilities of the quantum circuit C

Let us call the above "Average-case Task"

We know for the worst case circuit C, getting a multiplicative approximation for all y's with a BPP^{NP} algorithm would collapse PH

Let us call this the "Worst-case Task"

If we could show that "Average-case task" is as hard as the "Worst-case task" we would be done!

This is what we conjecture! Why do we believe this conjecture?

1. Some such reductions are known for #P-problems over finite fields since the 90's

2. We can prove it for Haar random circuit family with $(1 \pm \exp(-n))$-multiplicative error

That's why there is some optimism.

What about anticoncentration? We can actually show this for several families of random quantum circuits.

Final Remarks on Random Circuit Sampling

① Verification

Anticoncentration implies that typical probabilities are 2^{-n}

If $n = 50$ qubits, how can we verify that our experiment produces sample from the correct distribution and not uniform noise

Linear Cross-Entropy Benchmark

A statistical test to distinguish anti-concentrated distributions from uniform
Takes exponential time, so difficult to scale

① Collect a large # samples $y_1 \dots y_m$ from random circuit C

② Compute probability that quantum circuit outputs each y_i ⇒ Exponential time

③ Compute $\sum_{i=1}^{m} \frac{1}{m} \log \frac{1}{q_c(y_i)}$

④ Hope that m is large enough, so that the above converges to

$$\sum_{y \in \{0,1\}^{50}} q_c(y) \log \frac{1}{q_c(y)}$$

⑤ One can compute that this quantity is sufficiently different when C is the circuit vs uniform noise

② Noise

The above assumes that we can't hope to get a TV-error classical sampler from the output distribution of a simple but perfect quantum circuit

In reality, the quantum circuit also has noise. Does all the above still work?

This and verification are both very big bottlenecks in practice and a lot of research is going into these

You can look at the recent papers to get an idea of what the current status is

This concludes our discussion of quantum advantage
- How to establish it or rule it out?
- What sort of structure is needed?
- Practical and near-term considerations

Quantum Notions of NP

We are going to discuss quantum analogues of NP

These turn out to be connected to fundamental questions in quantum chemistry and condensed matter physics

Firstly, let us think of NP as a proof system

$x \in L \implies \exists$ proof/certificate $\pi \in \{0,1\}^{poly(|x|)}$ s.t. Verifier accept (x, π) always — Borrowing logic terminology, we call this Completeness of proof system which means "Every true statement can be proven"

$x \notin L \implies \forall$ proofs π, Verifier does not accept (x, π) — Soundness of proof system "No false statements can be proven"

Defining the quantum analogues of NP will require us to understand what happens when the verifier can use randomness

This defines a complexity class called MA which stands for "Merlin-Arthur"

$\boxed{\text{MA}}$ A language L is in MA if $\exists$ poly-time randomized verifier V

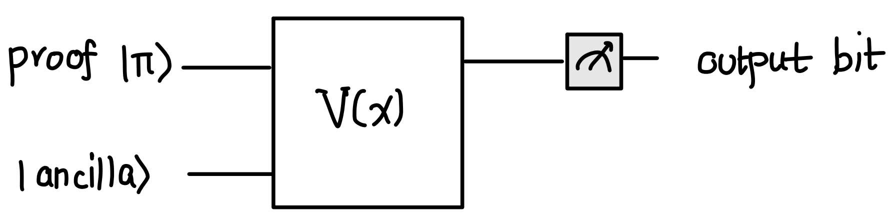
if $x \in L \implies \exists$ proof π s.t. $\mathbb{P}[\text{ V accepts } (x,\pi)] \geq 2/3 \implies$ Completeness

if $x \notin L \implies \forall$ proofs π $\quad \mathbb{P}[\text{ V}(x,\pi) \text{ accepts }] \leq \frac{1}{3} \implies$ Soundness

The name "Merlin-Arthur" comes from the tales of Camelot where Merlin is an all powerful wizard that can come up with any proof but King Arthur — who is poly-time bounded — has to check the proof since Merlin can't be trusted

A first attempt at generalizing MA to a quantum complexity class might be to make the verifier quantum. This gives us a complexity class called QCMA.

$\boxed{\text{QCMA}}$ A language L is in QCMA if $\exists$ poly-time (uniform) circuit family V(x)



such that

if $x \in L \Rightarrow \exists$ classical proof $\pi \in \{0,1\}^{poly(|x|)}$ s.t. $\mathbb{P}[\, V(x) \text{ accepts } \pi \,] \geq \frac{2}{3}$

if $x \notin L \Rightarrow \quad \forall$ proofs $\pi \quad \mathbb{P}[\, V(x) \text{ accepts } \pi \,] \leq \frac{1}{3}$

We could also make the proof to be an arbitrary quantum state $|\pi\rangle \in (\mathbb{C}^2)^{\otimes poly(|x|)}$
This defines the complexity class called

QMA

Putting other restrictions on the proof give us other complexity classes in between as we will see later

One can immediately see that NP $\subseteq$ MA $\subseteq$ QMA

To examine the probabibility that the verifier accepts on some proof $|\pi\rangle$ we shall need a more general notion of measurement called POVMs.

So far, we have looked at measuring if a qubit is 0 or 1 (or + or - in another basis)

Given a state $|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$

$$\mathbb{P}[\text{ first qubit of } \psi \text{ gives } 0 \text{ on measurement}] = \sum_{y \in \{0,1\}^{n-1}} |\alpha_{0y}|^2$$
$$= \Big\| \sum_{y \in \{0,1\}^{n-1}} \alpha_{0y} |y\rangle \Big\|^2$$

and similarly for $\mathbb{P}[\text{ measuring } 1] = \Big\| \sum_{y \in \{0,1\}^{n-1}} \alpha_{1y} |y\rangle \Big\|^2$

These are norms of the vector $|\psi\rangle$ after we have projected them on the subspaces spanned by computational basis states of the form
$\{|0y\rangle\}_{y \in \{0,1\}^{n-1}}$ and $\{|1y\rangle\}_{y \in \{0,1\}^{n-1}}$

You can describe the projector operator on these spaces by

$$\Pi_0 = |0\rangle\langle 0| \otimes \mathbb{I}_{n-1} \quad \text{and} \quad \Pi_1 = |1\rangle\langle 1| \otimes \mathbb{I}_{n-1}$$

Note that $\sum_{y \in \{0,1\}^{n-1}} \alpha_{0y} |y\rangle = \Pi_0 |\psi\rangle$

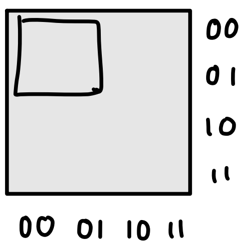
and $\mathbb{P}[\text{ first qubit is } 0] = \| \Pi_0 |\psi\rangle \|^2$

Now, $\mathbb{P}[\text{Verifier accepts } |\pi\rangle] = \| \Pi_1 U(|\pi\rangle|0\rangle^{\otimes a})\|^2$

$$= \langle\pi|\langle 0^a| (U^\dagger \Pi_1 U)|0^a\rangle|\pi\rangle$$

Suppose M was a matrix acting on 2-qubits $\quad M = \sum_{x,y\in\{0,1\}^2} M_{xy} |x_1 x_2\rangle\langle y_1 y_2|$

Then $\langle 0|M|0\rangle = \sum_{x_2, y_2 \in\{0,1\}} M_{0x_2,0y_2} |x_2\rangle\langle y_2|$

Pictorially, $M =$ 

$\langle 0|M|0\rangle =$ top left block of M

Similarly, $\langle 0^a| U^\dagger \Pi_1 U |0^a\rangle$ = Block of the matrix $U^\dagger \Pi_1 U$

Calling this block M_1, we have that $\mathbb{P}[\text{Verifier accepts } \pi] = \langle \pi | M_1 | \pi\rangle$

$$= \mathrm{Tr}[M_1 |\pi\rangle\langle\pi|]$$

POVM element

$\mathrm{Tr}(A) = \sum_i A_{ii} = \sum \lambda_i(A)$ is the trace function

$\langle A,B\rangle = \mathrm{Tr}[B^\dagger A] = \sum_{ij} \overline{B_{ij}} A_{ij}$ defines an inner product on matrices

Note that $\mathrm{Tr}(ABCD) = \mathrm{Tr}(DABC)$ and $\mathrm{Tr}(A\otimes B) = \mathrm{Tr}(A)\cdot\mathrm{Tr}(B)$

POVM (Positive Operator Valued Measurements)

A POVM $M_1, \ldots M_k$ is a set of operators satisfying

$M_i \succeq 0$ (M_i is a positive semidefinite matrix meaning

① $\forall$ all complex vectors x, $\langle x|M|x\rangle \geq 0$

OR equivalently

② $M_i = \sum_k \lambda_i(k) |k\rangle\langle k|$ where $\lambda_i(k) \geq 0$)

and $\sum_{i=1}^{k} M_i = I$

$\mathbb{P}[\text{Measuring } i^{th} \text{ operator on } |\pi\rangle] = \mathrm{Tr}[M_i |\pi\rangle\langle\pi|] = \langle \pi | M_i | \pi \rangle$

A special case of POVM $\{ M , I-M \}$ → Note that they sum to I

Any eigenvector $|v\rangle$ of M with eigenvalue λ
is also an eigenvector of $I-M$ with eigenvalue $1-\lambda$

So, one can diagonalize M and $I-M$ in the same basis

$$M = \sum_i \lambda_i |v_i\rangle\langle v_i|$$

Then $$I-M = \sum_i (1-\lambda_i) |v_i\rangle\langle v_i|$$

Naimark's Dilation Theorem — Every POVM can be expressed as a projective measurement (i.e. projection on subspaces) on a system tensored with some ancillary space.

For example, $\mathbb{P}[\text{Verifier accepts } |\pi\rangle] =$ Measure $|\pi\rangle$ with POVM $\{M, I-M\}$

or

Measure $|\pi\rangle \otimes |0^a\rangle$ with projectors $\{\Pi_1, \Pi_0\}$

We will not discuss POVM measurements for their own sake further

NEXT TIME — POVMs and Properties of QMA