LECTURE 11 (February 21)

TODAY Random Oracle Separation of BQP-search from BPP search

RECAP **Result** $\exists$ NP^O-search problem that is in BQP^O but not in BPP^O whp. over the choice of O

Yamakawa-Zhandry search problem Inverting a specific one-way function

Let Σ be an alphabet that we will choose to be $\mathbb{F}_q^n$ where q is a prime power with $q = O(n^2)$

$O : \Sigma \longrightarrow \{0,1\}$ be a random oracle

$C \subseteq \Sigma^n$ be a subspace of $(\mathbb{F}_q^n)^n$ that forms an error-correcting code with certain properties that we describe later

$\boxed{\text{Problem}}$ Let $f : C \longrightarrow \{0,1\}^n$ be defined as

$$f(c_1, \dots c_n) = (O(c_1), \dots O(c_n))$$

Domain is the set of codewords

Find a preimage of 0^n

Theorem Choosing C appropriately, whp over choice of O

(1) $\exists$ a quantum algorithm that can approximately prepare a uniform superposition over all solutions with poly(n) queries
i.e. it can prepare the state

$$\propto \sum_{x \in f^{-1}(0)} |x\rangle$$

(2) any classical algorithm requires 2^{n^c} queries to find a pre-image

This problem is in NP given access to the oracle [Why?]

How to choose C ? Assume that each symbol of the each codeword c is distinct

① **List Recoverability** : This will be helpful in ensuring classical hardness

② **Decoding from random errors in the dual code** This will be helpful in designing the quantum algorithm

Such codes exist

Quantum Algorithm

How to efficiently prepare the state

$$|\psi\rangle \propto \sum_{c \in C : f(c) = 0} |c\rangle \quad ?$$

Consider the following two states which can be efficiently prepared :

$$|1_C\rangle \propto \sum_{c \in C} |c\rangle \quad \text{and} \quad |1_{pre}\rangle \propto \sum_{x \in \Sigma^n : O(x) = 0^n} |x\rangle$$

Only supported on codewords

Only supported over 0^n preimages but over the entire alphabet Σ^n and not just the domain $C \subseteq \Sigma^n$

If we could somehow take $\underbrace{\text{pointwise product}}_{\text{Not a linear operation}}$ of these two states and normalize it we would be done !

Instead we will apply QFT

Quantum Fourier Transform QFT

Analogue of $H^{\otimes n}$ on larger alphabets

This is a unitary transformation that maps

$$QFT^{\otimes n} |x\rangle \longrightarrow \bigotimes_{i=1}^{n} \left(\frac{1}{\sqrt{|\Sigma|}} \sum_{y_i \in \Sigma} \omega_p^{\phi(x_i \cdot y_i)} |y_i\rangle \right)$$

Here, $x \in \Sigma^n$ where $\Sigma = \mathbb{F}_q^n$ where $q = p^r$ for prime p

Notation $\quad |f\rangle = \sum_x f(x) |x\rangle$ — amplitude in standard basis

Then, we denote by $|\hat{f}\rangle = QFT |f\rangle = \sum_x \hat{f}(x) |x\rangle$ — amplitude in Fourier basis

Two very useful properties of QFT

① Pointwise product becomes convolution after QFT [Exercise]

$$|f \cdot g\rangle = \sum_x f(x) g(x) |x\rangle$$

$$|\widehat{f \cdot g}\rangle = QFT^{\otimes n} | f \cdot g \rangle = \frac{1}{\sqrt{|\Sigma|^n}} \sum_x \hat{f} \star \hat{g}(x) |x\rangle \quad \text{where} \quad \hat{f} \star \hat{g}(x) = \sum_{y+z=x} \hat{f}(y) \hat{g}(z)$$

② QFT of uniform superposition over subspace C is uniform superposition over dual subspace $C^{\perp}$

$$\frac{1}{\sqrt{|C|}} \sum_{x \in C} |x\rangle \xrightarrow{QFT^{\otimes n}} \frac{1}{\sqrt{|C^{\perp}|}} \sum_{x \in C^{\perp}} |x\rangle$$

where $C^{\perp} = \{ d \mid c \cdot d = 0 \ \forall c \}$

Back to the quantum algorithm

How to efficiently prepare the state

$$|\psi\rangle \propto \sum_{c \in C : f(c)=0} |c\rangle \ ?$$

Consider the following two states :

$$|1_C\rangle = \frac{1}{\sqrt{|C|}} \sum_{c \in C} |c\rangle \quad \text{and} \quad |1_{pre}\rangle \propto \sum_{x \in \Sigma^n : O(x)=0} |x\rangle$$

We want to take pointwise product of $|1_C\rangle$ & $|1_{pre}\rangle$ (and normalize)

Suppose we apply QFT, $\underbrace{\text{take convolution}}$ and apply inverse QFT

Not a unitary or linear operation in general

$$|1_C\rangle \otimes |1_{pre}\rangle \xrightarrow{QFT^{\otimes n} \otimes QFT^{\otimes n}} \underbrace{\left(\sum_z \hat{1}_C(z)|z\rangle\right)}_{\text{unif. over } C^\perp} \otimes \left(\sum_e \hat{1}_{pre}(e)|e\rangle\right)$$

$$= \sum_{\substack{c \in C^\perp \\ e \in \Sigma^n}} \hat{1}_C(c)\, \hat{1}_{pre}(e)\, |c\rangle|e\rangle$$

$$\xrightarrow[|x\rangle|e\rangle \to |x\rangle|x+e\rangle]{U_{add}} = \sum_{\substack{c \in C^\perp \\ e \in \Sigma^n}} \hat{1}_C(c)\, \hat{1}_{pre}(e)\, |c\rangle|c+e\rangle$$

Now $c \in C^\perp$ is a dual codeword and treating e as an error

Suppose we could correct the error, i.e. $\forall c \in C^\perp$, $\mathrm{Decode}_{C^\perp}(c+e) = c$

Making this a unitary $U_{decode}\ |c\rangle|c+e\rangle \longrightarrow |c - \mathrm{Decode}(c+e)\rangle|c+e\rangle$

If Decode was always correct, then

$$\xrightarrow{U_{decode}} \sum_{\substack{c \in C^\perp \\ e \in \Sigma^n}} \hat{1}_C(c)\, \hat{1}_{pre}(e)\, |0\rangle|c+e\rangle = \sum_z \underbrace{\left(\sum_{c+e=z} \hat{1}_C(c)\, \hat{1}_{pre}(e)\right)}_{= \hat{1}_C * \hat{1}_{pre}(z)} |0\rangle \otimes |z\rangle$$

Now we have managed to perform convolution in the Fourier space

Applying an inverse QFT

$$\xrightarrow{I\otimes (QFT^{-1})^{\otimes n}} = \sqrt{|\Sigma|^n} \sum_z 1_C(z)1_{pre}(z)|0\rangle|z\rangle$$

$$\propto |0\rangle \otimes \Big(\sum_{\substack{z\in C \\ \& f(z)=0^n}} |z\rangle \Big)$$

Now all this is assuming the ideal scenario where we can decode the dual code perfectly

[Why is the above not possible?]

In general, one can only decode it w.h.p. under some type of error and implement the above circuit with some error

<u>What sort of errors?</u> The errors come from QFT of $|1_{pre}\rangle$

$$|1_{pre}\rangle \propto \sum_{x\in\Sigma^n:\ O(x)=0^n} |x\rangle = \Big(\sum_{\substack{x_1\in\Sigma \\ O(x_1)=0}} |x\rangle \Big) \otimes \Big(\quad \Big) \otimes \cdots \Big(\sum_{\substack{x_n\in\Sigma \\ O(x_n)=0}} |x\rangle \Big)$$

Since $O:\Sigma\to\{0,1\}$ is a random oracle, typically $1/2$ of Σ is "colored" with 0

What is the QFT of $\Big(\sqrt{\frac{2}{|\Sigma|}} \sum_{\substack{x_1\in\Sigma \\ O(x_1)=0}} |x\rangle \Big)$?

To understand let us consider the Hadamard example again, i.e. $\Sigma=\{0,1\}^n$

If we have $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \xrightarrow{H^{\otimes n}} |0\rangle^{\otimes n}$

Now suppose we color each $x\in\{0,1\}^n$, "RED" OR "BLUE" w.p. $1/2$ each

and consider $\frac{1}{\sqrt{|RED|}} \sum_{x\in RED} |x\rangle \xrightarrow{H^{\otimes n}} \sum_{e\in\{0,1\}^n} \beta(e)|e\rangle$ where β depends on the coloring

What do we get here?

In the exercises, you will be asked to show that

$$\mathop{\mathbb{E}}_{\substack{RED/BLUE \\ \text{coloring}}} \big[|\beta(e)|^2 \big] = \begin{cases} \frac{1}{2} & \text{if } e=0^n \\ \frac{1}{2}\cdot\frac{1}{2^n-1} & \text{if } e\neq 0^n \end{cases}$$

Thus, we get something that looks like $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}} \sum_{e\neq 0} \frac{1}{\sqrt{2^n-1}} |e\rangle$ on average over choice of RED/BLUE (upto signs)

Over the alphabet Σ, we get something similar, i.e. typically

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}\sum_{\substack{e\neq 0\\ e\in\Sigma}} \frac{1}{\sqrt{|\Sigma|-1}}|e\rangle$$ on average over choice of $\mathcal{O}$ (upto phases)

Thus, $QFT^{\otimes n}|1_{pre}\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}\sum_{\substack{e\neq 0\\ e\in\Sigma}} \frac{1}{\sqrt{|\Sigma|-1}}|e\rangle\right)^{\otimes n}$

Now, recall that we want to apply U_{decode} to $\sum_{\substack{c\in C^\perp\\ e\in\Sigma^n}} \hat{1}_c(c)\,\hat{1}_{pre}(e)|c\rangle|c+e\rangle$

One can think of $QFT^{\otimes n}|1_{pre}\rangle$ as a superposition over errors

If we measure each symbol of the error, with probability $\frac{1}{2}$ we get $e=0$ (no error)

with probability $\frac{1}{2}$ we get e to be a random shift

Overall, each coordinate of the codeword c is corrupted independently

And typically half of the coordinates are corrupted

If our code can corrupt such errors with high probability, we can implement the above "ideal" algorithm approximately

Concretely, what we want

Consider a random error e sampled as follows

$$\mathbb{P}[e_i = 0] = \frac{1}{2}$$

$$\mathbb{P}[e_i = z] = \frac{1}{2(|\Sigma|-1)} \quad \forall z\in\Sigma\setminus\{0\}$$ for each coordinate independently

Then, we want a decoding algorithm $\mathrm{Decode}_{C^\perp}$ s.t.

$$\mathbb{P}_e\left[\forall c\in C^\perp : \mathrm{Decode}_{C^\perp}(c+e) = c\right] = 1-2^{-\Theta(n)}$$

Lower Bound for Classical Algorithms

For this, we need another property of the code

① List Recoverability : This will be helpful in ensuring classical hardness

suppose we fix $S_1, S_2, \dots, S_n \subseteq \Sigma$ where $|S_i| \le 2^{\sqrt{n}}$

and consider codewords $c \in \Sigma^n$ where $c_1 \in S_1$
$c_2 \in S_2$
$\vdots$
$c_n \in S_n$

Then, # such codewords should be $\le 2^{n^{3/4}}$

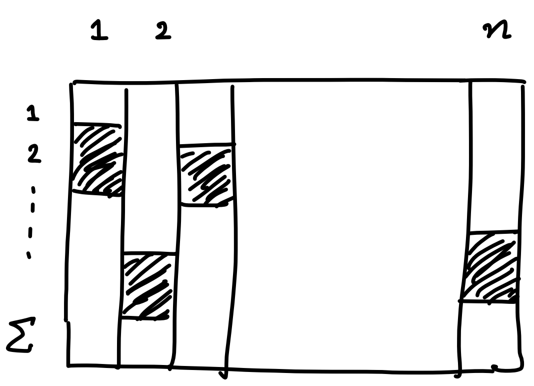
To simplify the argument we will assume that the algorithm is non-adaptive
i.e. it decides at the beginning all queries it is going to make

The proof works also for adaptive algorithms with a small modification of the argument

Assume that the algorithm outputs $c_1, \dots, c_n$ as a preimage of 0^n with $2^{\sqrt{n}}$ queries
Then, we may assume that algorithm queries $O(c_1), O(c_2), \dots, O(c_n)$ [Why?]

So, the picture looks like this for the first coordinate
the algorithm queries S_1, for the second it queries S_2
and so on where each $|S_i| \le 2^{\sqrt{n}}$

In picture,



Where ▨ denotes the queries algorithm makes

Note that $|\Sigma| \approx 2^{O(n^2)}$ and

There are at most $2^{n^{3/4}}$ codewords consistent with ▨
One of these is the output

$$\mathbb{P}_O[\text{ any of these is a preimage of } 0^n] = 2^{n^{3/4}} \cdot 2^{-n} = 2^{-c \cdot n}$$

Near-term Quantum Advantage

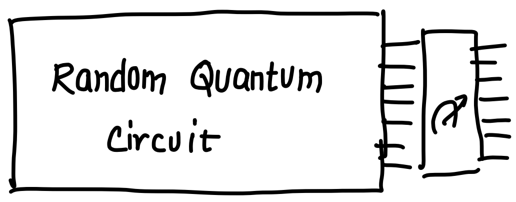
YZ-search problem is in BQP^O not in BPP^O } provable quantum advantage & we can instantiate with a cryptographic hash function

& in NP^O } verifiable in poly-time by classical algorithms

But the problem is that the quantum circuit to solve it can't be implemented on current quantum devices which are noisy & limited to small-depth computation

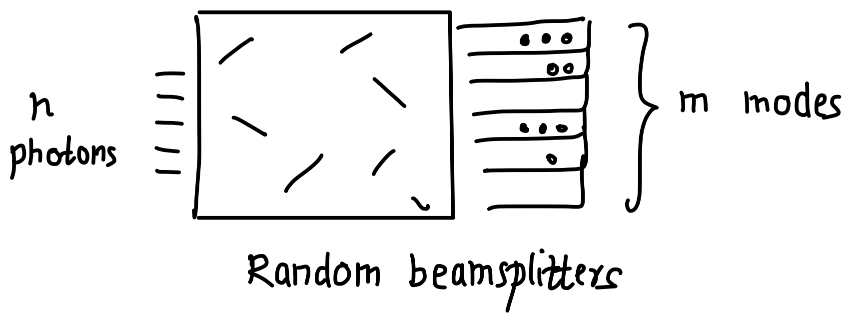
Near-term experiments are based on random circuit or boson sampling

Random Circuit Sampling



Given a random quantum circuit obtained from a "simple" family, sample from the output distribution

Boson sampling



Sample from output distribution of boson sampling experiment

These are near-term, we have some evidence of quantum advantage, although there is still a lot we don't know but not verifiable easily

Holy-grail = Provable quantum advantage + Near-term + Verifiable

Now we are going to focus on Random Circuit Sampling & consider what evidence of quantum advantage do we have. We won't cover boson sampling here

Note : Both these tasks are practically useless (except for maybe generating randomness) but for now we want to demonstrate quantum advantage experimentally

Warning : This is a rapidly evolving field and we are only going to talk about some initial results.

Practically, it is not clear whether the evidence is robust in the presence of noise and whether we have effectively demonstrated quantum advantage since these experiments are hard to scale & verify

Sampling from the output distribution of a quantum circuit is #P-hard

↳ as hard as counting number of solutions of a SAT formula

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\, |\varphi(x)\rangle$$

SAT-formula

↳ output qubit

$$\mathbb{P}[\text{ output is } 1] = \frac{\#\text{ satisfying assignments}}{2^n}$$

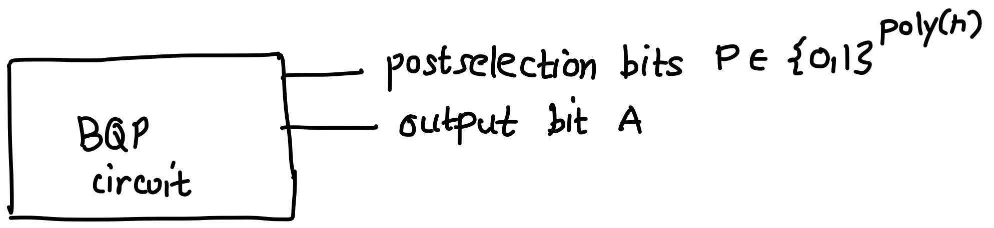
This seems promising but we need simpler classes of quantum circuits and need that this is robust to errors & noise which exact sampling is not

<u>Dream Conjecture</u> There exists a simple family of quantum circuits s.t. approximating $|\langle y|C|0^n\rangle|^2$ for most outcomes $y\in\{0,1\}^n$ is #P-hard when C is drawn at random

This ignores noise in the quantum circuit which is also something one has to take into account

In order to do this, we need the notion of postselection & the complexity class postBQP

<u>PostBQP</u>



A problem is in postBQP if (1) $\mathbb{P}[\underset{P}{\text{postselection bits}} = 0\cdots 0] \geq 2^{-poly(n)}$

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

We are conditioning on an event of exponentially small probability

This is not physically viable but is a very powerful theoretical tool

Postselection gives a lot of computational power

$\boxed{NP \subseteq postBQP}$ $$|\psi\rangle = \sqrt{1-\varepsilon}\left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |\varphi(x)\rangle\right) + \sqrt{\varepsilon}\,|abort\rangle|1\rangle$$

SAT formula; special state

↳ $= 0.01/\sqrt{2^n}$

If we postselect on 2^{nd} qubit being 1,

$$\text{unnormalized } |\psi\rangle = \frac{\sqrt{1-\varepsilon}}{\sqrt{2^n}} \sum_{x:\,\varphi(x)=1} |x\rangle + \sqrt{\varepsilon}\,|abort\rangle$$

If φ is unsatisfiable measuring first register gives abort

Otherwise in the worst-case φ has a single satisfying assignment x^* so the unnormalized state is

$$\frac{\sqrt{1-\varepsilon}}{\sqrt{2^n}} |x^*\rangle + \sqrt{\varepsilon}\, |\text{abort}\rangle$$

$$\approx \frac{1}{\sqrt{2^n}} |x^*\rangle + \frac{0.01}{\sqrt{2^n}} |\text{abort}\rangle$$

$\mathbb{P}[\text{we measure } x^*] \geq 0.99$

We can define the classical version postBPP similarly and the above also works for postBPP

$\boxed{\text{Theorem}}$ postBQP = PP $\longrightarrow$ problems where random algorithms do slightly better than random guessing

postBQP $\leq$ PP follows from just minor modifications to the BQP $\subseteq$ PP proof we saw earlier

The other direction is non-trivial and was shown by Aaronson

We are not going to cover the proof in the lecture but I might try to make an exercise out of it

$\boxed{\text{Theorem}}$ postBQP = postBPP $\Longrightarrow$ PH collapses to the third level

Proof follows from a bunch of known complexity results which I don't expect everyone to know, so we are going to take it for granted

Now the punchline is, you can take a simple quantum circuit class C

for example, IQP circuits which look like $H^{\otimes n} D H^{\otimes n}$ where D is a diagonal unitary in the computational basis

These circuits are way less powerful than BQP but if we give them the power of postselection, they become as powerful as postBQP

$\boxed{\text{Theorem}}$ $\quad$ postIQP = postBQP

Now, if there was an exact classical sampler to sample from output distribution for an IQP circuit, then we could classically postselect and

$$\text{post BPP} = \text{postIQP} = \text{post BQP} \implies \text{PH collapses}$$

These circuits cannot solve many problems but for the specific problems they solve, a classical computer could not solve them unless PH collapses

Caveats ① We have shown existence which says in the worst-case sampling from an IQP circuit is hard classically but if it was a single pathological case, it may not be useful experimentally

Can we say that on average this task is hard?

② Again the above assumes exact sampler which is again not experimentally feasible

Can we say that this is still hard if the classical sampler samples from a distribution that is ε-close in total variation distance?