Lecture 16

Nov 19, 2024

Pf. Consider a (yes) instance of QCIRCUIT SAT.

i.e. $\exists\ |\psi\rangle$ s.t. $C(|\psi\rangle)$ accepts w pr $\geq 1-\epsilon$.

Then let $$|\Psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi, 0^m\rangle$$

the History state of $|\psi\rangle$. By construction,

$\langle\Psi| H_{prop} |\Psi\rangle = 0$

$\langle\Psi| H_{in} |\Psi\rangle = 0 \qquad \Rightarrow \qquad \langle\Psi|H|\Psi\rangle \leq \epsilon.$

$\langle\Psi| H_{out} |\Psi\rangle \leq \epsilon$

What about a (no) instance of QCircuit SAT?

Recall the max success prob. of a QCircuitSAT instance was $\cos^2\Theta$ where Θ was the angle between $\mathbb{1}_{2^n} \otimes |0\rangle\langle 0|^m$ and $C^\dagger (|1\rangle\langle 1| \otimes \mathbb{1}_{2^{n+m-1}}) C$ projectors.

If max success prob is small $(\leq \epsilon)$ then Θ is large (near $\frac{\pi}{2}$).

as $\cos^2\Theta = \epsilon$.

We want to show that $\lambda_{min}(H)$ is not super small.

Since $H_{prop} \geq \frac{c}{T^2}(\mathbb{1} - \Pi_{prop})$

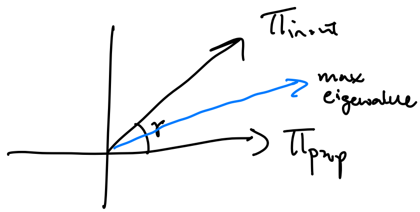
it suffices to show lower bound on:

$$\lambda_{min}\left(\frac{c}{T^2}(\mathbb{1} - \Pi_{prop}) + (\mathbb{1} - \Pi_{inout})\right)$$

$$\gtrsim \frac{c}{T^2}\lambda_{min}\left((\mathbb{1} - \Pi_{prop}) + (\mathbb{1} - \Pi_{inout})\right)$$

$$\gtrsim \frac{c}{T^2}\left(2 - \lambda_{max}(\Pi_{prop} + \Pi_{inout})\right)$$

$$= \frac{c}{T^2}\left(2 - 2\cos^2\frac{\gamma}{2}\right) = \frac{2c}{T^2}\sin^2\frac{\gamma}{2}.$$



where γ = angle between Π_{prop} and Π_{inout}

To do this, let's bring back

$$V = \sum_{t=0}^{\tau} |t\rangle\langle t| \otimes g_t \cdots g_1.$$

We know that

$$V^\dagger \Pi_{prop} V = \text{projector onto states} \left\{ |h_\psi\rangle := \frac{1}{\sqrt{T+1}} \sum_{t=0}^{\tau} |t\rangle \otimes |\psi\rangle \right\}$$

$$V^\dagger \Pi_{\text{in+out}} V = \left(|T\rangle\langle T| \otimes C^\dagger \left(|1\rangle\langle 1|_1 \otimes \mathbb{1} \right) C \right) \cdot \left(|0\rangle\langle 0| \otimes \mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m| \right)$$

terms commute.

$$\gamma = \text{angle}\left(\Pi_{\text{prop}}, \Pi_{\text{in+out}} \right) = \text{angle}\left(V^\dagger \Pi_{\text{prop}} V, V^\dagger \Pi_{\text{in+out}} V \right)$$

To calculate angle between spaces:

$$\cos^2 \gamma = \max_{|\psi\rangle} \langle h_\psi | \Pi_{\text{in+out}} | h_\psi \rangle$$

$$= \max_{|\psi\rangle} \frac{1}{T+1} \sum_{t=0}^{1} \langle t | \langle \psi | \Pi_{\text{in out}} | t \rangle | \psi \rangle$$

$$= \max_{|\psi\rangle} \frac{T-1}{T+1} + \frac{1}{T+1} \Big(\langle \psi | C^\dagger \left(|1\rangle\langle 1| \otimes \mathbb{1} \right) C | \psi \rangle + \langle \psi | \mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m| \, | \psi \rangle \Big)$$

$$= \frac{T-1}{T+1} + \frac{1}{T+1} 2 \cos^2 \frac{\theta}{2}$$

as optimal $|\psi\rangle$ is midway between projectors $C^\dagger(|1\rangle\langle 1|_1 \otimes \mathbb{1})C$

and $\mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m|$ which are θ apart.

Recall $\sqrt{\epsilon} = \cos\theta = 2\cos^2\frac{\theta}{2} - 1 \Rightarrow$

$\Rightarrow 2\cos^2\frac{\theta}{2} = 1-\sqrt{\epsilon} \Rightarrow$

$$\cos^2\gamma = \frac{T-1}{T+1} + \frac{1}{T+1}\left(1+\sqrt{\epsilon}\right) = 1 - \frac{(1-\sqrt{\epsilon})}{T+1}.$$

$$\sin^2\frac{\gamma}{2} = \frac{1-\cos^2\gamma}{2} = \frac{1-\sqrt{\epsilon}}{2(T+1)}.$$

Therefore, $\lambda_{min}(H) \geq \frac{2c}{T^2}\left(\frac{1-\sqrt{\epsilon}}{T+1}\right) = \Omega\left(\frac{1}{T^3}\right)$

for small ϵ.

So if yes instance, $\lambda_{min}(H) \leq \epsilon$

if no instance, $\lambda_{min}(H) \gtrsim \frac{1}{T^3}$.

To complete pf of QMA-hardness, first use amplification to convert any QCIRCUITSAT problem to $(1-\epsilon, \epsilon)$ amplification for $\epsilon < \frac{1}{T^3}$. Then apply the circuit-to-Hamiltonian construction.

A more sophisticated analysis proves that no instances map to $\Omega\left(\frac{1}{T^2}\right)$.

Note that we only proved QMA-hardness for $O(\log T) = O(\log n)$ local Hamiltonians. Your homework includes a transform to 5-local Hamiltonians.

This will yield a Hamiltonian acting on $T+n+m$ qubits.

Also, we only proved it was QMA-hard to estimate $\lambda_{min}(H)$ to $\frac{1}{T^3} \sim \frac{1}{N^3}$ where N is the number of qubits in the Ham.

It may be easier to get a coarser approximation

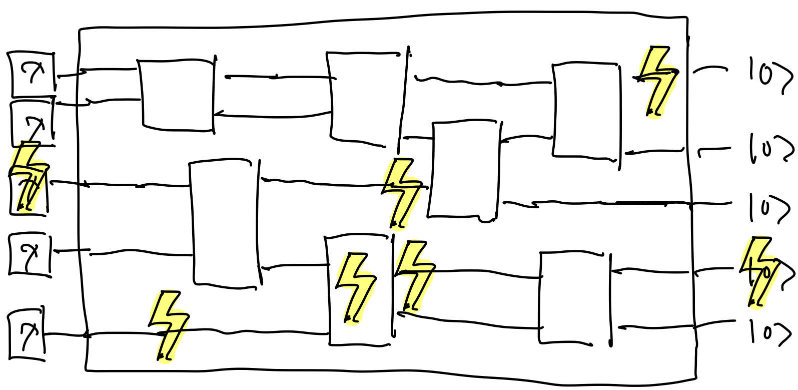
Quantum Error Correction.

Until know, we have talked about perfect application of gates and perfect initializations of q. states.

What if that is not the case?

Error-correction gives a theory of how to recover information in the presence of noise.

Biggest block to our construction of large scale q. computers.
Quantum computation is more succeptible to noise than classical computation.



Errors can occur in <u>any</u> component...

How do we correct.

① A theory of correction for static q. information.

No computation occuring, just errors.

Run a sequence of corrections to return information back to original.

Quantum analog of reliable data storage.

Classical: CDs, SSDs, Harddrives, Pen and Paper

② Correction interspersed with computation

Called Fault-Tolerance and will be covered in Lecture 20 by guest lecturer Michael Beverland.

How do we correct classical information?

Theory: Rich. Practice: Redundancy.

WiFi/3G/4G : LDPC codes

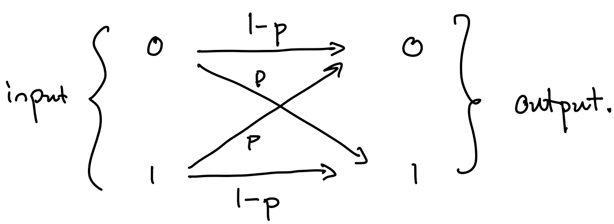
CD-Rom: Reed-Solomon codes

Computation: Run it thrice and take majority vote.

Reasonable because a classical bit in a modern transistor incurs an error with $pr < 10^{-18}$.

To analyze error-correction (theoretically), we first need a model for error.

Simplest model bit flip channel.



$$\rho \longmapsto \mathcal{E}(\rho) = p \cdot X \rho X + (1-p)\, \rho.$$

Notion holds for quantum also.

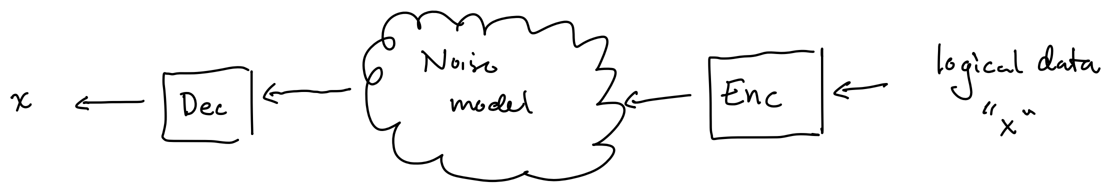
High level: A channel is a map from density matrices to density matrices consistent with q. mechanics axioms.

Bit flip on each bit:

$\mathcal{L}(\mathbb{C}^{2^n}) \ni \rho \longmapsto \mathcal{E}^{\otimes n}(\rho)$.

$\Pr[\text{no bit gets flipped}] = (1-p)^n \to 0$ as $n \to \infty$.

General procedure.



Easiest classical example: Repetition code.

$$\bar{0} := \mathrm{Enc}(0) = 0\ldots\ldots 0$$

$$\bar{1} := \mathrm{Enc}(1) = \underbrace{1\ldots\ldots 1}_{n \text{ times}}.$$

Assume $p < \frac{1}{2}$.

$$\mathrm{Dec}(y) = \begin{cases} 0 & \text{if } |y| < \frac{n}{2} \\ 1 & \text{if } |y| > \frac{n}{2} \end{cases} .$$

$$\Pr_{\text{error}}\left[\text{decoding is wrong}\right] = \Pr_{\text{error}}\left[\geq \frac{n}{2} \text{ bits flipped}\right] \leq e^{-\Omega(n)}$$

The 3 troubles of quantum error correction.

① Infinite collection of possible errors even just on one qubit.

② No-cloning theorem.

There is no unitary mapping $|0\rangle \mapsto |0\rangle|0\rangle$ and $|+\rangle \mapsto |+\rangle|+\rangle$

Therefore quantum repetition code doesn't make sense.

③ Measurements destroy quantum info.

How do we correct when measurement is perturbative?

Today: Shor's 9 qubit code + theory of EC.

Let's correct first for a specific subset of errors:

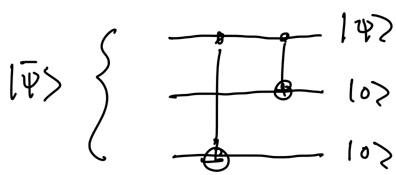
Single qubit X (bit flip), Z (phase flip), and XZ (bit + phase)

To correct just bit flip errors, appeal to classical intuition.

map $|0\rangle \mapsto |000\rangle$
$|1\rangle \mapsto |111\rangle$

Does not violate no cloning as we copy in 1 basis

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longmapsto |\bar{\psi}\rangle = \mathrm{Enc}|\psi\rangle = \alpha|000\rangle + \beta|111\rangle.$$

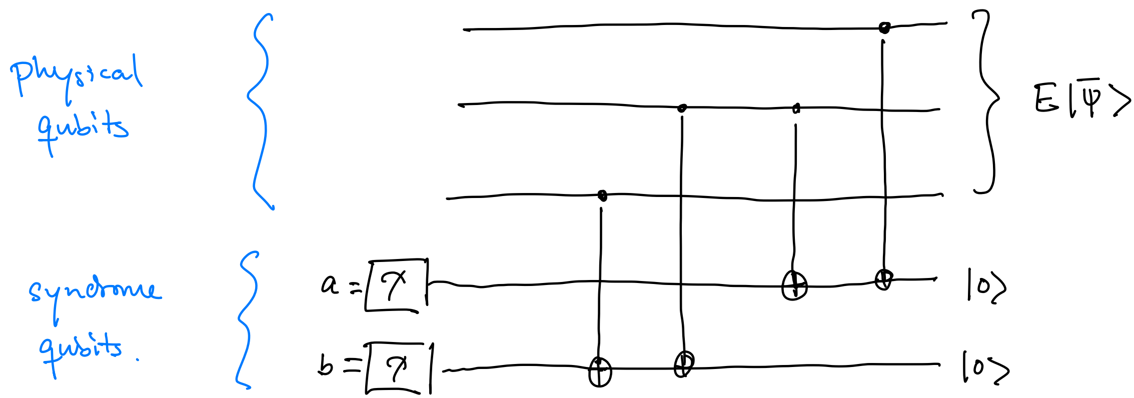


Say error occurs on middle qubit.

$$E|\bar{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle.$$

Measuring would destroy superposition.

Instead, we compute error-syndromes and measure these.



If run on $|x, y, z\rangle$, then $a = x \oplus y$, $b = y \oplus z$.

$$a \oplus b = x \oplus z.$$

By linearity, when run on $E|\bar{\Psi}\rangle = \alpha|010\rangle + \beta|101\rangle$

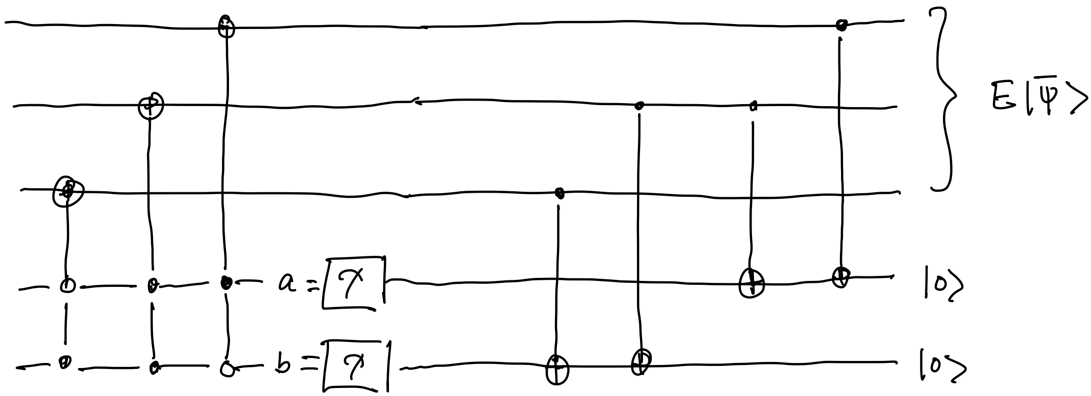
we get

$$\alpha|010\rangle|11\rangle + \beta|101\rangle|11\rangle$$

$$= \left(E|\bar{\Psi}\rangle\right) \otimes \underbrace{|11\rangle}_{\text{syndrome}}.$$

What happens for other bit flip errors?

Error	a	b
no error	0	0
1st qubit	1	0
2nd qubit	1	1
3rd qubit	0	1



After correction, we can discard the syndrome qubits (they are now unentangled by measurement).

$$\boxed{Dec = Enc^{-1} \circ Correction}.$$