6.S979 Lecture 20

- Project topic due today by email
- Let me know over Thanksgiving break if you think you want to present

Last time: Pauli Braiding Test

A prob verifier can force A & B to share $|EPR^{\otimes n}\rangle$ and measure $X(a)$, $Z(b)$

Today: Delegated quantum computation using PBT [Grilo '17]

Prelude: a slight extension of PBT

Instead of measuring $X(a)$ to obtain $y \in \{0,1\}$

Ask for X basis measurement on each qubit i s.t. $a_i = 1$

$b \in \{0,1\}^n$ outcomes

$$y = \langle b, a \rangle$$

Obs: Pauli measurements on EPR are computationally easy to simulate

A hard problem for BQP

Warmup: $P \subseteq NP$

Circuit C

transcript

Prover $\longrightarrow$ Verifier

$t=0,\ 0 \dots\dots 0$
$t=1,\ 1 \dots\dots 0$
$t=2,\ 1 \dots 1 \dots 1\ 0$
$\vdots$

$t=T \; \ldots \; 1$

output bit

Aside: This is how you show 3SAT or graph coloring are NP-complete

You can do a quantum version of this

$BQP \subseteq QMA$

"quantum NP"

Q. circuit C

$|\psi_c\rangle$

Prover $\longrightarrow$ Verifier

q. transcript

trying to "show" that C accepts $|0\rangle$ w/ $p \geq 0.9$

$$|\psi_c\rangle = \frac{1}{\sqrt{T}} \sum_{t=1}^{T} |t\rangle |\psi_t\rangle$$

History state (Feynman Kitaev)

Can check history state by measuring H_c ← "history Hamiltonian"

- If $C|0\rangle$ accepts w/ $p > 0.9$ then $\langle \psi_c | H_c | \psi_c \rangle \leq E_c$

- If $C|0\rangle$ accepts w/ $p < 0.1$ then $\forall\ |\psi\rangle$, $\langle \psi | H_c | \psi \rangle \geq E_s$

- $E_s - E_c \geq \frac{1}{\text{poly}(n)}$

$$H_c = \sum_i H_i$$

$$H_{\text{input},j} = \underbrace{|0\rangle\langle 0|}_{\text{clock}} \otimes |1\rangle\langle 1|_j$$

$$H_{\text{prop.}} = \frac{1}{2}\left(|t+1\rangle \otimes I - |t\rangle \otimes U_t\right)\left(\langle t+1| \otimes I - \langle t| \otimes U_t^{\dagger}\right)$$

t'th gate

$$|\psi_C\rangle \xrightarrow{\text{span}\{|t\rangle, |t+1\rangle\}} |t\rangle|\psi_t\rangle + |t+1\rangle U_t|\psi_t\rangle$$

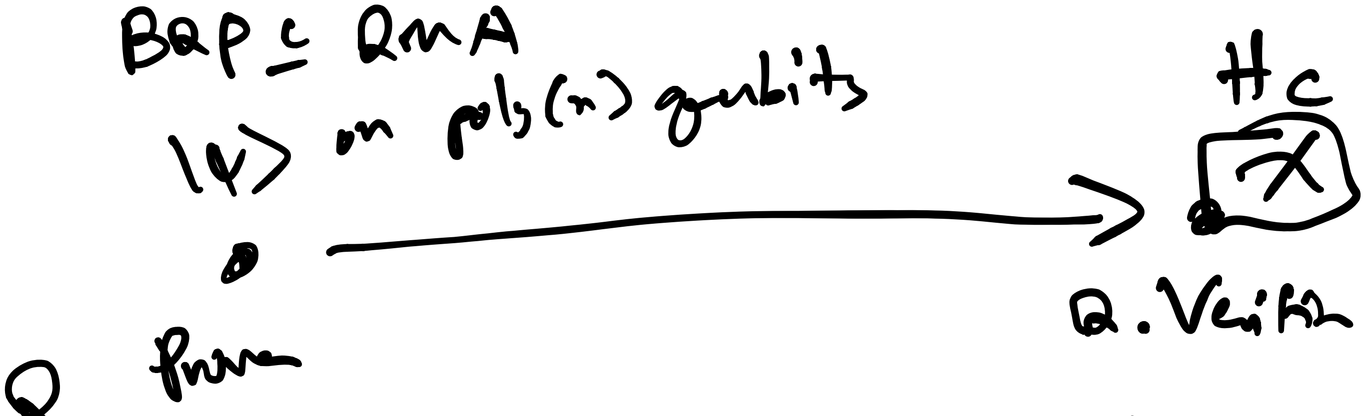
$$H_{output} = |T\rangle\langle T|_{clock} \otimes |NO\rangle\langle NO|_{output}$$

By some clever tricks, you write $H_C = \sum H_i$ (e.g. perturbative gadgets)

H_i: tensor product of X, Z, I

- - - - - - - - - - - - - - - -

BQP $\subseteq$ QMA

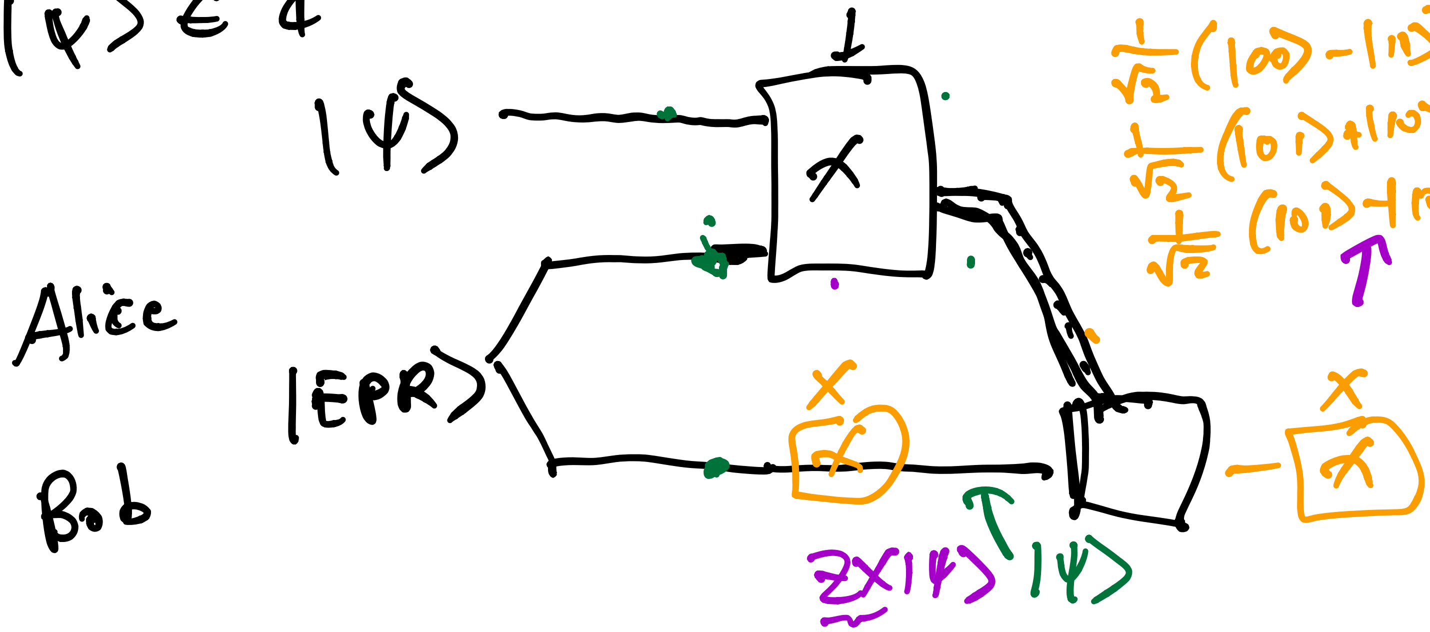


Want to convert to

Enter Quantum Teleportation:

$|\psi\rangle \in \mathbb{C}^2$

Bell basis = $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, $\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$



Obs: Bell basis = $\{|EPR\rangle, (I\otimes Z)|EPR\rangle, (I\otimes X)|EPR\rangle, (I\otimes XZ)|EPR\rangle\}$

Obs: Suppose Bob wants measure X or Z on $|\psi\rangle$.

Turns out he can measure first, then apply correction from Alice

- Suppose B. measures X, correction is X

$$\langle\psi|X X_f X|\psi\rangle = \langle\psi|X|\psi\rangle$$

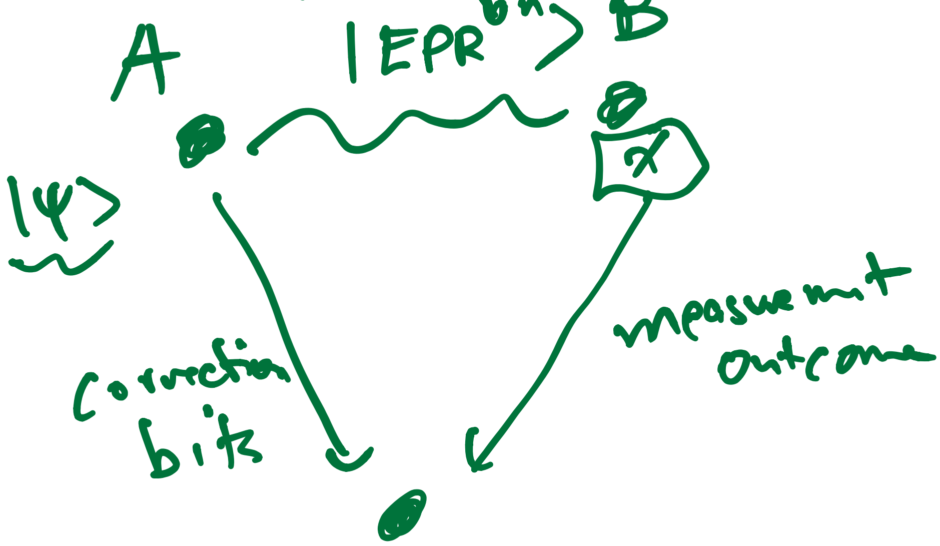
correction is Z

$$\langle\psi|Z\,X\,Z|\psi\rangle = -\langle\psi|X|\psi\rangle$$

so B. has to flip outcome

same for corr = XZ

Consequence



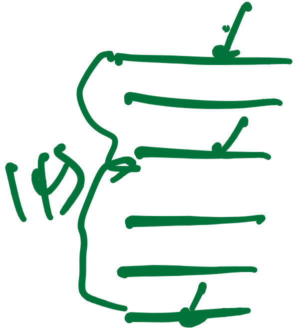
Cl. verifier corrects the measurement outcomes

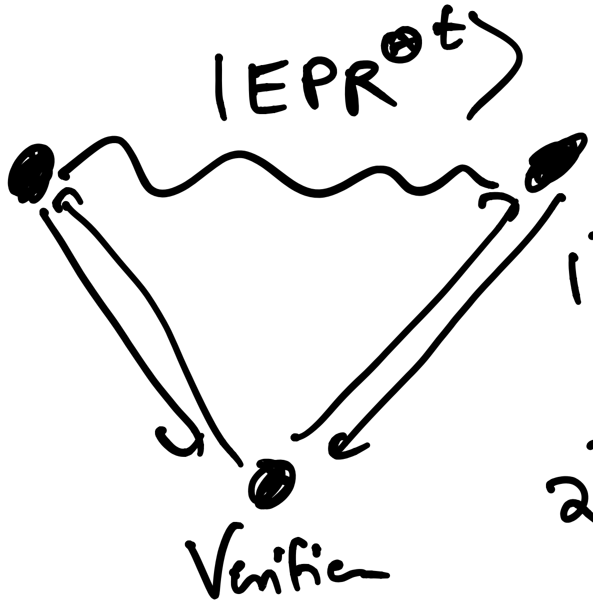
Putting it all together:

$$BQP \subseteq MIP^*$$

Circuit C on n qubits $\longrightarrow$ H_C on poly(n) qubits n'

$t = \text{poly}(n) \gg n'$





V. either:

1) Runs PBT

2) "Energy test"

- V. samples n locations in $1 \ldots t$ and sends them to Alice
- Samples a Pauli operator $\sim H_c$ sends to Bob
- Receive correction bits from A measurement outcomes from B'

Conclusion: V's result from energy test is obtained from measuring H_i on whatever $|\psi\rangle$ A chose to teleport

$$H_c = \sum_i H_i$$

- Accept if outcome is -1, reject if $+1$

$\Pr[V_{\text{accepts}}] \propto \langle\psi| H_c |\psi\rangle$

YES: $\exists\, |\psi_c\rangle$, $\langle\psi_c|H_c|\psi_c\rangle \le E_c$

NO: $\forall\, |\psi\rangle$, $\langle\psi|H_c|\psi\rangle \ge E_s$

$\Rightarrow$ If C accepts w.h.p., $\exists$ strat for A, B that is accepted in the protocol w/ $p \ge p_c$ $\leftarrow$ depends on E_c

If C rejects w.h.p., $\forall$ strat for A, B, $p_{\text{acceptance}} \le p_s$ $\leftarrow$ depends on E_s

Ultimately, want $p_c \ge 2/3$, $p_s \le 1/3$

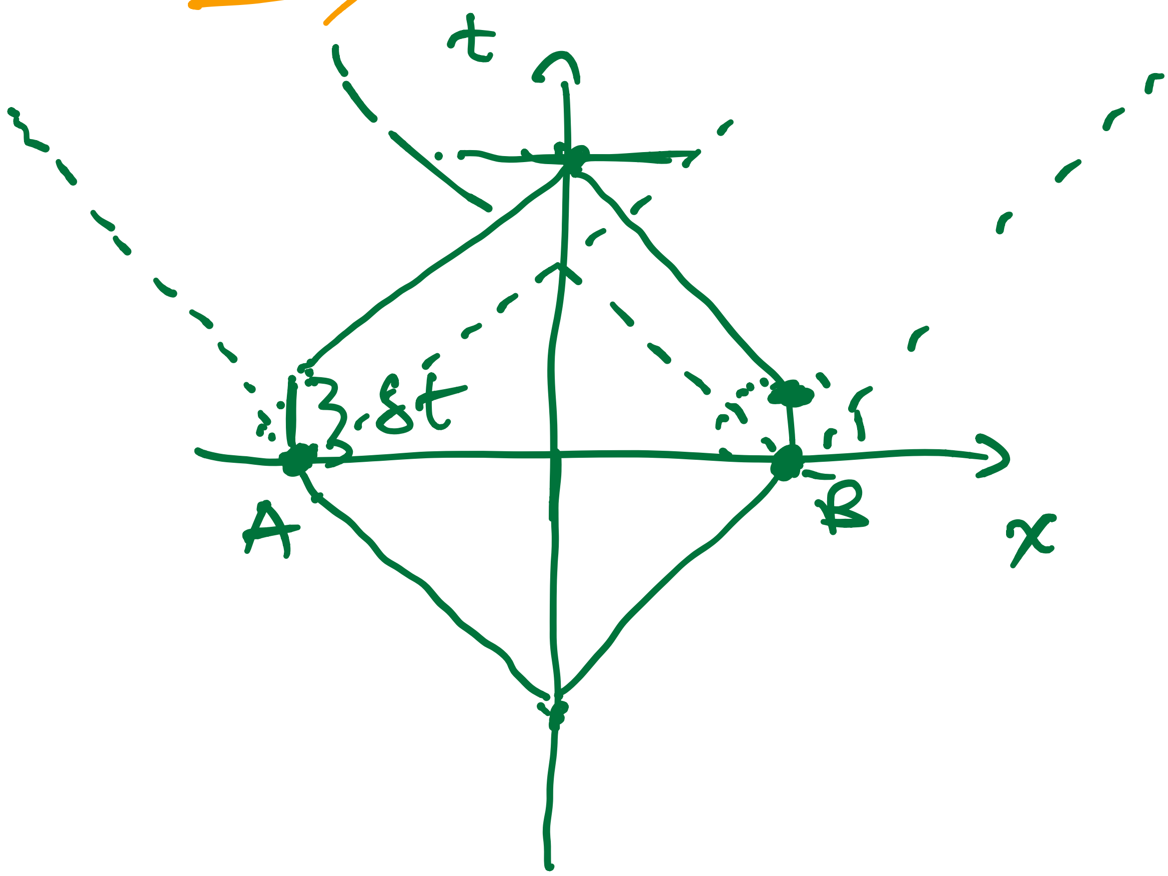
Can achieve using

- "amplification" of H_c by taking $H_c^{\otimes k}$
- parallel repetition of protocol

We showed

$$BQP \subseteq MIP^*$$

- Note: this is trivially true b/c $BQP \subseteq PSPACE = IP$.
- <u>However:</u> this protocol has <u>efficient provers</u>
- One-round protocol $\implies$ relativistically secure



- Disadvantage: polynomial overhead
  C of size n
  protocol requires poly (n)
  Bottleneck is H_C

Verifier on a leash get a protocal w/ $O(n \log n)$ resources required

- Not blind: Alice has to know what C is

- Two provers: (Mahadev & follow ups address this).