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

Last time: Paul: Braiding Test
A pub verifier can force \( A \) \& \( B \)
to share \( \ket{EPR^\otimes n} \) and measure \( X(a), Z(b) \)

Today: Delegated quantum computation using \( \text{PBT} \)
[ Grilo '17 ]
Prelude: a slight extension of PT

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

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

be $90/13^n$ extremal

$y = \langle b, a \rangle$

---

Obs: Pauli measurements on EPR are computationally easy to simulate

A hard problem for BQP

Warmup: $P \leq NP$

Circuit $C$

transcript

\[
\begin{array}{c}
\text{Prover} \quad t \leq 0, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{Verifier} \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{false, } 0, 1, \ldots, 0 \\
\end{array}
\begin{array}{c}
\text{true, } 1, \ldots, 0 \\
\end{array}
\]
Aside: This is how you show 3SAT or graph coloring are NP-complete.

You can do a quantum version of this: $BQP \subseteq QMA$.

Q. circuit $C$

Trying to show that $C$ accepts $|0\rangle$ with $P \geq 0.9$.

$14_c^\uparrow \rightarrow 0$

Prover

g. transcript Verifier

$14_c^\uparrow = \frac{1}{\sqrt{T}} \sum_{t=1}^{T} |1_t^\uparrow) 14_t^\uparrow)$

History state (Feynman-Kitaev)
Can check history state by measuring $H_c$ - "history Hamiltonian"

- If $|G10\rangle$ accepts $\forall p > 0.9$
  then $\langle \psi_c \mid H_c \mid \psi_c \rangle \leq E_c$

- If $|G10\rangle$ accepts $\forall p < 0.1$
  then $\forall \langle 14 \rangle$, $\langle 4 \mid H_c \mid 4 \rangle \geq E_s$

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

$H_c = \sum_i H_i$

$H_{\text{input}_j} = 10\rangle\langle 01 \rangle \otimes 1i\rangle\langle i1 |$

$H_{\text{prop.}} = \frac{1}{2} (1_{t+1} \otimes I - 1_t \otimes U_t)$

$= (1_{t+1} \otimes I - \langle t1 \otimes U_t^+ \rangle)$
\[ |\psi_c\rangle \rightarrow \text{span}\{|H\rangle, |H + D2\rangle\}

\begin{align*}
|t\rangle & \equiv |\psi_4\rangle + \text{i} t_4 |\psi_3\rangle
\end{align*}

\[ H_{\text{output}} = |T\rangle\langle T|_{\text{each}} \otimes |\text{NO}\rangle\langle \text{NO}|_{\text{output}} \]

By some clever tricks, you write \[ H = \sum H_c \uparrow \]

\text{tensor product of } X, Z, I

BAP + QMA

|\psi\rangle \text{ on } \rho_{15}(n) \text{ qubits}

Q. From

Q. From

Q. From

\[|\psi\rangle \rightarrow \text{Want to convert to} \]

Q. From

Cl. Verify

Want to convert to

Q. From

Q. From

\[ H_c \]

Cl. Verify
Quantum Teleportation:

Enter: \( |v\rangle \in \mathbb{C}^2 \)

Bell basis: \( \frac{1}{\sqrt{2}} (|10angle + |01\rangle) \)

Alice: \( |EPR\rangle \)

Bob's XZ basis: \( \{ |EPR\rangle, |I0EPR\rangle, |I0EPR\rangle, |I0EPR\rangle \} \)

Suppose Bob wants to measure \( X_0Z \)

Obs: \( |\psi\rangle \)

Suppose Bob measures \( X \), then apply \( \sigma_X \).

Turn but he can measure first, \( \text{comet} \) is \( X \).

Bob measures \( X \), \( \langle 41X14 | 41X14 \rangle = \langle 41X14 | 41X14 \rangle = \langle 41X14 | 41X14 \rangle = \langle 41X14 | 41X14 \rangle \)

Obs: 41

Obs: 14

Alice and Bob share a quantum state \( |\psi\rangle \) which is entangled.
Conjecture is Z

\[ \langle \psi | Z \times Z | \psi \rangle = -\langle \psi | X \times X \rangle \]
so B. has to flip outcome

same for case \( X \times Z \)

---

**Consequence**

A \( \rightarrow \) EPR \( \rightarrow \) B

-intervention

\( | \psi \rangle \rightarrow \) measurement outcome

Cl. verifier corrects the measurement outcomes

---

Putting it all together:

\( \text{BQP} \subseteq \text{MIP} \)

Circuit \( C \) on \( n \) qubits

\[ H_c \text{ on } \text{poly}(n) \text{ qubits} \]

\[ t \cdot \text{poly}(n) \gg n \]
1. \( \text{EPR}^{\text{obs}} \)

2. "Energy test"

- \( V \) samples in locations in \( 1 \ldots t \) and sends them to Alice

- Samples a Pauli operator \( \sigma_i \) sends to Bob

- Receive correction \( \sigma_i \) from Alice, measurement outcomes from \( B' \)

Conclusions: \( V \)'s result from energy test is obtained from measuring \( \sigma_i \) on what \( |\psi\rangle \) A chose to teleport

\[ H_c = \sum_i H_i \]

- Accept if outcome is \( -1 \), reject if \( +1 \)

\[ \text{Pr}(V\text{accept}) \propto \langle 41 | H_c | 14 \rangle \]
Yes: \( \exists 1 \psi_c \), \( \langle 4_c | H_c | 4_c \rangle \leq E_c \)

No: \( \forall 1 \psi \), \( \langle 4 | H_c | 4 \rangle \geq E_s \)

\( \Rightarrow \) If \( C \) accepts w.h.p., \( \exists \) strat for \( A, B \) that is accepted in the protocol \( w/ P \geq P_c \) \( \text{depends on } E_c \)

If \( C \) rejects w.h.p., \( \forall \) strat for \( A, B \), \( p_{\text{accept}} \leq P_s \) \( \text{depends on } E_s \)

Ultimately, want \( P_c \geq \frac{2}{3} \), \( P_s \leq \frac{1}{3} \)

Can achieve using
- "amplification" of \( H_c \) by taking \( H_c \otimes k \)
- parallel repetition of protocol
We showed $\text{BQP} \leq \text{MIP}^*$

- Note: this is trivially true b/c $\text{BQP} \leq \text{PSPACE} = \text{IP}$
- However: this protocol has efficient provers

- One-round protocol relativistically secure
- **Disadvantage**: polynomial overhead
  of size $n$
  protocol requires $\text{poly}(Cn)$
  Bottleneck is $\mathbb{F}_C$

Verifier on a leash gets
a protocol with $O(Cn \log n)$ resources
required

- **Not blind**: Alice has to know
  what $C$ is

- **Two provers**: (Mahadev and
  follow up this address)