No class next week (Thanksgiving break)

Last time: Used PBT to delegate a quantum computation
\[ \text{BQP} \subseteq \text{MIP}^* \] (efficient provers)

Today: Use (failing) PBT to delegate an MIP protocol
\[ \text{NEXP} \subseteq \text{MIP}^* [g \leq \log(n), a = \text{poly}(n)] \]

Protocol parameters:
\[ \text{MIP} [q, a] \]
- Question length
- Answer length

? \[ \text{NEXP} \subseteq \text{MIP} [\text{poly}(n)] \]
Upper bound on MIP:

\[ \text{MIP}[p_{olb}(n), p_{olb}(n)] \]
\[ \implies \text{d! strategy can be described in } \exp(n) \text{ bits} \]
\[ \implies \text{MIP}[p_{olb}(n), p_{olb}(n)] \subseteq \text{NEEXP} \]

\[ \text{MIP}[\log(n), p_{olb}(n)] \subseteq \text{NP} \]
\[ \implies \text{MIP}^*[\log(n), p_{olb}(n)] \supseteq \text{NEEXP} \]

\[ \text{NEEXP} \subseteq \text{MIP}^*[\text{poly}(n), \text{poly}(n)] \]
\[ [N, Wright] \]
Fancy PBT:

Recall: Verifier can force prover to show $|EPR^0_n\rangle$, measure in $X$ or $Z$ basis

$q = \log(n)$

$a = poly(n)$

One can show: $E$ protocol with same guarantee ($X$ or $Z$ measurements on $|EPR^0_n\rangle$)

$q_b = \log(n)$, $a = poly(n)$

"gnomon low-degree test"

PBT +/- the BLR substring replaced by a test for the low-degree code
"Compiling" a protocol w/ QLD

Suppose you have a protocol $G$ that's works with "Pauli strategies":

A \text{ EPR}^n \rightarrow B

\begin{align*}
\psi
\end{align*}

\begin{align*}
\text{"X-basis measurement"}
\end{align*}

\begin{align*}
\alpha &= \text{ the outcome of X-basis measurement}
\end{align*}

\begin{align*}
\alpha' &= \text{ outcome of any measurement}
\end{align*}

\begin{align*}
\text{"X-basis"}_x
\end{align*}

\begin{align*}
M_{\alpha, \alpha'} = |\langle \alpha_x | \otimes | \alpha'_{x'} \rangle |
\end{align*}

Then $G'$ works for arbitrary $\mathcal{G}$ processes:

\begin{align*}
G' = \begin{cases} 
\frac{1}{3} & \text{QLDR} \\ \text{consistency}
\end{cases}
\end{align*}
\[ g[q, a] \rightarrow g'[q + \log(n), a + \text{polys}(n)] \]

Compression by introspection

Q. key distribution
Randomness expansion

\( a \rightarrow z \quad a \in \{0, 1\} \_

\text{Today: apply this idea to MIP* protocol}
Say $G$ is an MIP protocol with $q = \text{polys}(n)$, $a = \text{polys}(n)$, $x, y \sim \{0, 1\}^n$. 

```
Alice
    Q_A
    ▼
  A          B
    ▼
A, B \in \{X, Z\}^n
```

```
Bob
    Q_B
    ▼
B
    ▼
B, B \in \{X, Z\}^n
```

```
V(A, B|Q_A, Q_B)
```

```
\text{EPR}_{x, y}
```

```
Q_A \in \{0, 1\}^n \times \{0, 1\}^n
Q_B \in \{0, 1\}^n \times \{0, 1\}^n
```

```
\text{``X-basis''}                     \text{``Z-basis''}
```

```
Potential worry:

After obtaining $Q_A$, Alice could do more measurements on residual $q_i$ state to learn something about $Q_B$.
This is impossible: An X-basis measurement of a qubit “destroys” Z-basis information

\[ |E_{pr}\rangle = |00\rangle + |11\rangle \]

\[ \downarrow \text{Alice measures in X basis to get } + \]

\[ |1\rangle' = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \]

\[ \downarrow \text{Bob measures to get 1} \]

\[ |1\rangle \otimes |1\rangle \]

Suppose \( S \) has questions

\[ Q_A = \underbrace{\nu \in \{0, 13\}}_{11} \]

\[ Q_B = \underbrace{\nu, \nu \in \{0, 13\}}_n \]
\[ u' \in \mathbb{Z} \xrightarrow{EPR^0} \mathbb{Z} \rightarrow u \]

\[ u' \in \mathbb{Z} \xrightarrow{EPR^0} \mathbb{Z} \rightarrow v \]

**Problem:** Alice could have sneakily measured 2nd block of EPRs and learnt \( v \).

The \( X \)-basis outcome \( u' \) certifies that Alice didn't peek to \( v \).

---

\( NEXP \) is the line-point test.

\[ MDP = NEXP \]

\[ \text{colinear} \rightarrow \text{nonlinear} \]

\[ m \times f \]
Alice's Q: \( u \in \mathbb{F}_q^m \)

Bob's Q: \( l = \frac{1}{2} u + \lambda v : \lambda \in \mathbb{F}_q^3 \)

"Canonical description" of \( l \)

\( \text{"Scrambled intercept"} \; u \mod v \)
\[ u' = u + \lambda v \]

\[ \text{Note: pretend } \mathbb{P}_z = \mathbb{P}_2 \]

\[ X(v) \rightarrow \text{outcome be } \alpha, \beta \]

\[ \text{Example: } n=2, u, u', v \in 50, 13^2 \]

\[ (0,0) \xrightarrow{\mathbb{D}} \begin{array}{c} z^2 \text{ EPR } \theta^2 \end{array} \]

\[ \text{junk} \xrightarrow{\mathbb{D}} \begin{array}{c} X \text{ EPR } \theta^2 \end{array} \]

\[ v = (1,1) \]
\[ |\psi\rangle = |0,0\rangle_A \otimes |0,0\rangle_B \]
Bob measures \[ X(n) = X \otimes X \]
eigenstates of \[ X \otimes X \]
\[ b = +1 : \frac{1}{\sqrt{2}} (|100\rangle + |111\rangle), \frac{1}{\sqrt{2}} (|101\rangle + |110\rangle) \]
\[ b = -1 : \frac{1}{\sqrt{2}} (|100\rangle - |111\rangle), \frac{1}{\sqrt{2}} (|101\rangle - |110\rangle) \]
\[ |\psi_{w,\lambda}\rangle = \frac{1}{\sqrt{2}} \sum_{b=\pm 1} (-1)^b \lambda (|w + \lambda v\rangle) \]
\[ |\psi\rangle = |100\rangle_A \otimes \frac{1}{\sqrt{2}} (|100\rangle + |111\rangle) \]

Pf: (super sketchy):

You know from QLD that $X \in \mathbb{Z}$ basis measurements are already done.
Prove that \([M_{w',b}^v, \mathcal{X}(w)] = 0\)

\[
a \leftarrow X \xrightarrow{z} M_{w',b}^v
\]

\[
b = a \cdot v
\]

\[\implies \text{NEXP} \leq \text{MIP}^* [\log(n) \text{poly}(n)] \text{ vs. } \text{NP} = \text{MIP} [\log(n), \text{poly}(n)]\]