Last time: Use entanglement to "compress" a protocol

|X| = N

1X| = log(n)

"Question reduction":

"Answer reduction":
We know \( \text{MIP} = \text{NEXP} \)

Delegating to provers using an MIP protocol

Issues:
- To compute \( V(A,B,x,y) \), need to know \( A,B,x,y \) and only verifier can learn all these things

For now: everything is classical

\[ V : \ V(A,B,x,y) = \text{YES} \]

\[ A' \neq A \land B' \neq B \]
Completeness: follows if Alice can simulate Bob on question y

Soundness: follows from analysis of C-V game

Now we can delegate V
We want Alice to prove to us:
- She possesses A, B, s.t.
  \[ V(A, B, x, y) = \text{YES} \]
- Her \( A \sim B \) matches Bob's \( A' \sim B' \).

Unfortunately, only know how to give proofs for NP/\text{NEXP} statements

Recall what the MDP=\text{NEXP} protocol for graph coloring looks like:

\[ G \]

\[ \text{Alice} \quad \text{Bob} \]

\[ E(\text{coloring}) \quad E(\text{coloring}) \]

\[ E(x, y) \quad E(x_2, y_2) \]

\[ E(x_1, y_1, z_1, \ldots) \quad \text{Verify} \]
Obs: If $A \oplus B$ succeed in this protocol,
- $\exists$ coloring for $\Sigma$
- $A \oplus B$ both possess $\exists$ (coloring) and answer accordingly some for $A \oplus B$

$\exists (A)_{\frac{2}{\varepsilon}}, \exists (B)_{\frac{2}{\varepsilon}}$

Checks that $\exists (A), \exists (B)_{\frac{2}{\varepsilon}}$

are consistent with $V(\Sigma, \Sigma, x, \delta) = \text{YES}$

Checks that $\exists (A)_{\frac{2}{\varepsilon}} = \exists (A')_{\frac{2}{\varepsilon}}$

"PCP of proximity" "PCP composition"

"assignment tester"
Hastad's PCP: 3 bits for a prefix \( \Pi \) let you certify that \( \Pi \) is a valid NP proof

Protocol compression to show

\[ \text{MIP}^* = \text{RE} \]

Protocol: 2 Turing machines

- "Sampler" generates questions \( xy \) for provers

- "Decider" checks whether answers are correct

Parametrized by \( n \)

\( S, D \) run in time \( \text{poly} (n) \)

\[ V = (S, D) \quad \forall n \]

Parameters:

- Time \( (S, n) \) "question length"
- Time \( (D, n) \) "answer length"
\[
\mathcal{E}(\nu_n, \alpha) := \min \text{ dimension of state that achieves success prob. } \geq \alpha \text{ on protocol } \nu_n
\]

\[\mathcal{E}(\text{CHSH}, \alpha) \geq 2 \quad \text{for } \alpha > \frac{3}{4}\]

\[\mathcal{E}(\text{CHSH}, \alpha) = \infty \quad \alpha \leq \cos^2(\pi/8)\]

\# qubits = \log(d)

\[\mathcal{E}(\text{CHSH}, \alpha) = 0 \quad \alpha \leq \frac{3}{4}\]

\text{Compression theorem: } \exists \text{ Compress: }

\text{Suppose } \nu = (S, D) \text{ is "normal form"}

Then \text{ Compress}(\nu) = \nu^{\text{cor}} = (S^{\text{cor}}, D^{\text{cor}})

- \text{TIME}(S^{\text{cor}}, n), \text{TIME}(D^{\text{cor}}, n) = \text{poly}(n)
- Your "simulates" \( \mathcal{V}^{2^n} \)

Completeness: If \( \mathcal{V}^{2^n} \) has a perfect strategy, so does \( \mathcal{V}^n \)

Soundness: If \( \omega^* (\mathcal{V}^{2^n}) \leq \frac{1}{2} \), then

\[
\omega^* (\mathcal{V}^{\text{cop}}}^{n}) \leq \frac{1}{2}
\]

- \( 3(\mathcal{V}^{\text{cop}}}^{n}, \frac{1}{2}) \geq \max \{3(\mathcal{V}^{2^n}, \frac{1}{a}), 2^{2^n} \cdot c \cdot 3 \} \)

\( O(2^n) \) EPR pairs to generate random questions

Design an MDP* protocol for the halting prob. (complete for RE)

Recall: Halting prob. is given T.M. \( M \) determine whether \( M \) halts on \( 0 \) input
Define Turing machine \( F \):

\[ F : \text{Inputs:} \quad \langle R, M, n, x, y, a, b \rangle \]

1. Run \( M \) for \( n \) steps, accept if it halts.

2. Compute "D": Run \( R \) on input \( \langle R, M, n, x, y, a, b \rangle \)

3. Compute sampler "S"

\[
\text{Compute \quad \text{Compress} \left( \langle S, D \rangle \right) = \langle \text{Compress} \left( S \right), \text{Compress} \left( D \right) \rangle}
\]

4. Accept if \( \text{Compress} \left( n, x, y, a, b \right) \) accepts

Define \( D_{\text{halt}} = F \left( \langle F, M \rangle, \ldots \right) \)
Input T.M "M"

1) First run M for 2^n steps.
   If halt, accept
2) Else, run compressed version of yourself.

Why does \( \mathcal{V} \) halt solve the halting problem?

1) Completeness: If \( M \) halts, then there exists a perfect strategy for \( \mathcal{V} \) halts.
Suppose $M$ halts in time $T$
then $\omega^*(\nu_{halt}^T) = 1$
(Decider automatically accepts)
then by completeness of recursion
\[ \omega^*(\nu_{halt}^T) = \omega^* (\text{compress}(\nu_{halt}^T)) \]
\[ = \omega^* (\nu_{halt}^T) = 1 \]
\[ \Rightarrow \omega^* (\nu_{halt}^T) = 1 \]

Soundness: If $M$ doesn't halt,
then $\omega^* (\nu_{halt}^T) < \frac{1}{2}$

Suppose contrary. Then

\[ 2 (\nu_{halt}^T, \frac{1}{2}) \]
\[ \geq \max \{ 2, 3(\nu_{halt}^T, \frac{1}{2}) \}, 2^{2n} \]
\[ \geq \ldots \quad 2^{2n} \]