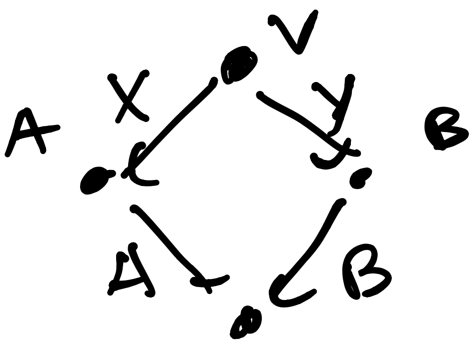
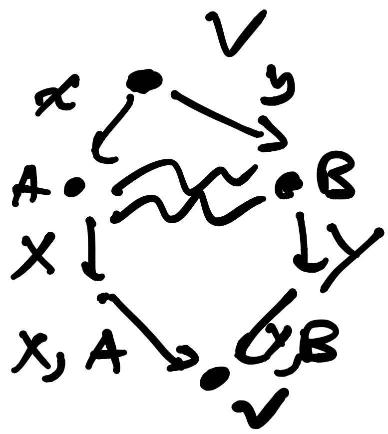
6.S979 Lecture 22

- Let me know if you want to speak on 12/9
- ncSoS/NPA demo Tuesday 12/1 3pm eastern

Last time: Use entanglement to "compress" a protocol



$\Longrightarrow$



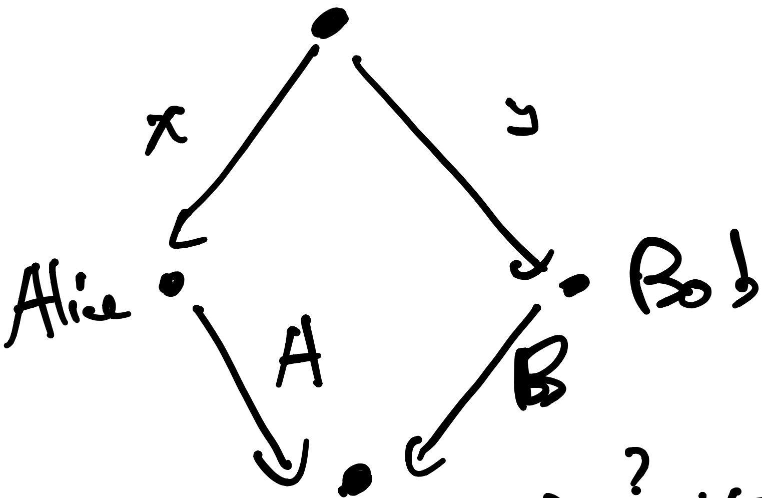
$|X| = N$ $\qquad$ $|x| = \log(n)$

"Question reduction"

"Answer reduction":

We know

MIP = NEXP



$V(A, B, x, y) \stackrel{?}{=} \text{YES}$

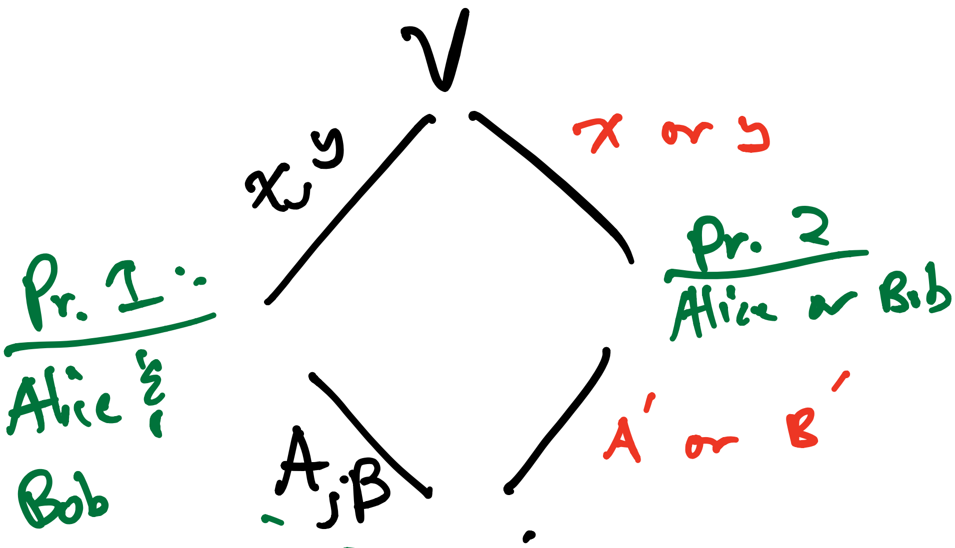
poly(|A|, |B|)

delegate 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 ←



"oracularization"

cf. clause-var game

com. test

V: $V(A, B, x, y) \stackrel{?}{=} \text{YES}$

$A' \stackrel{?}{=} A$ or $B' \stackrel{?}{=} B$

Completeness: follows b/c Alice can simulate Bob on question y

Soundness: Follows from analysis of C-V game

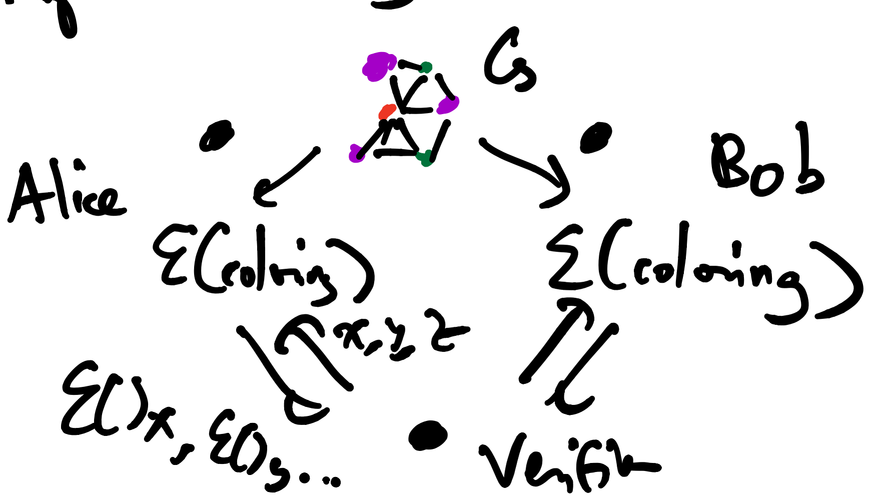
Now we can delegate V

We want Alice & Bob to prove to us:

- She possesses A, B, s.t. $V(A, B, x, y) = YES$
- Her A or B matches Bob's A' or B'.

Unfortunately, only know how to give proofs for NP/NEXP statements

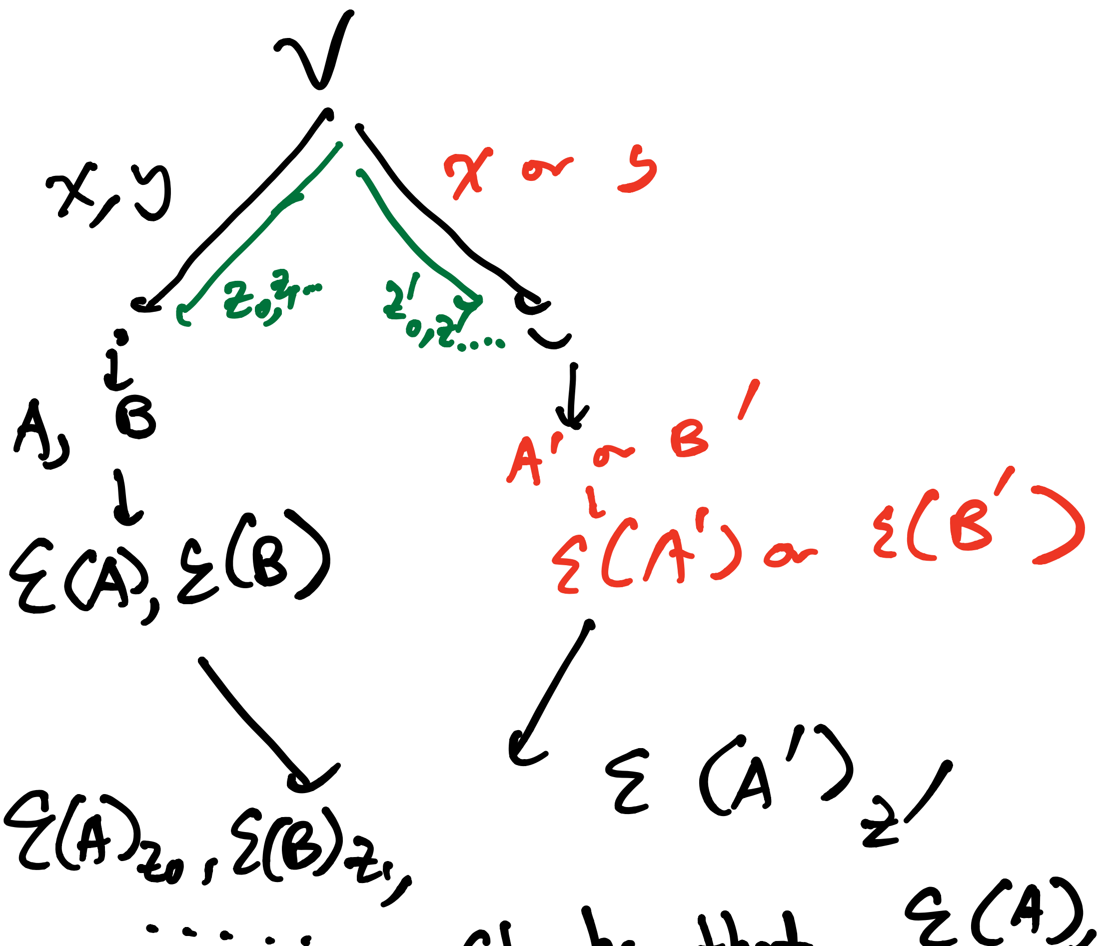
Recall what the MIP=NEXP protocol for graph coloring looks like:



Obs: If A & B succeed in this protocol.

- $\exists$ coloring for G
- A & B both possess $\mathcal{E}$(colorings) and answer accordingly

same for A & B



Checks that $\mathcal{E}(A), \mathcal{E}(B)\big|_z$ are consistent w/ $V(A, B, x, y) = \text{YES}$

Checks that $\mathcal{E}(A)\big|_z \stackrel{?}{=} \mathcal{E}(A')\big|_{z'}$

"PCP of proximity" "PCP composition"

"assignment tester"

Håstad's PCP: 3 bits from a pf. string Π lets you certify that Π is a valid NP proof

Protocol compression to show

$MIP^* = RE$

Protocol: 2 Turing machines

- "Sampler" S generates questions x, y for provers

- "Decider" D checks whether answers are correct

Parametrized by n

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

$V = (S, D)$ $\quad V_n$

Parameters: $\mathrm{TIME}(S, n)$ "question length"

$\mathrm{TIME}(D, n)$ "answer length"

$\mathcal{E}(\mathcal{V}_n, \alpha) :=$

min dimension of state that achieves success prob. $\geq \alpha$ on protocol $\mathcal{V}_n$

e.g. $\mathcal{E}(\text{CHSH}, \alpha) \geq 2$ for $\alpha > 3/4$

qubits $= \log(d)$

$\mathcal{E}(\text{CHSH}, \alpha) = \infty$ $\alpha > \cos^2(\pi/8)$

$\mathcal{E}(\text{CHSH}, \alpha) = 0$ $\alpha \leq 3/4$

<u>Compression theorem</u>: $\exists$ Compress:

Suppose $\mathcal{V} = (S, D)$ is "normal form"

- S looks like fine-pt. dist.
- Opt. strategy only needs EPR
- ....

Then Compress$(\mathcal{V})$

$= \mathcal{V}^{comp} = (S^{comp}, D^{comp})$

- TIME(S^{comp}, n), TIME$(D^{comp}, n) = \text{poly}(n)$

- $\mathcal{V}_n^{comp}$ "simulates" $\mathcal{V}_{2^n}$

__Completeness:__ If $\mathcal{V}_{2^n}$ has a perfect strat., so does $\mathcal{V}_n^{comp}$

__Soundness:__
- If $\omega^*(\mathcal{V}_{2^n}) \leq 1/2$, then $\omega^*(\mathcal{V}_n^{comp}) \leq \cancel{1/2}$

- $\mathcal{E}(\mathcal{V}_n^{comp}, \frac{1}{2}) \geq \max\{\mathcal{E}(\mathcal{V}_{2^n}, \frac{1}{2}), 2^{2^n \cdot c}\}$

original strat for $\mathcal{V}_{2^n}$

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

Design an MIP* 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 $\mathcal{F}$:

$\mathcal{F}$: Inputs: "R", "M", n, x, y, a, b

decider for a protocol → input for halting prob.

1. Run M for n steps, accept if halts.

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

3. Compute sampler "S"

Compute Compress("S", "D")

$= "\mathcal{V}^{comp}" = ("S^{comp}", "D^{comp}")$

4. Accept if $D^{comp}(n,x,y,a,b)$ accepts

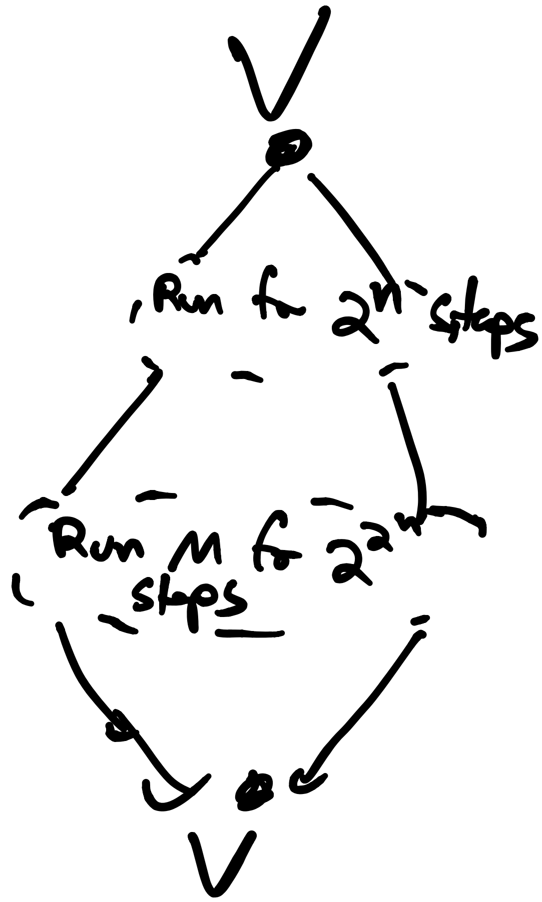
Define $D^{halt} = \mathcal{F}("\mathcal{F}", "M", \dots)$

Input T.M "M"

1) First run M for n steps.
If halt, accept

2) Else, run compressed version of yourself.

or



Why does V^{halt} solve the halting problem? :

1) Completeness: If M halts, then $\exists$ perfect strat. for V^{halt}.

Suppose M halts in time T

then $\omega^*(\mathcal{V}^{halt}_T) = 1$

(Decider automatically accepts)

then by completeness of compression

$$\omega^*(\mathcal{V}^{halt}_{\log(T)}) = \omega^*((\mathrm{Compress}(\mathcal{V}^{halt})_T)$$

$$= \omega^*(\mathcal{V}^{halt}_T) = 1$$

$$\Longrightarrow \quad \omega^*(\mathcal{V}^{halt}_n) = 1$$

<u>Soundness:</u> If M doesn't halt,

then $\omega^*(\mathcal{V}^{halt}_n) < 1/2$

Suppose contrary. Then

$$\mathcal{E}(\mathcal{V}^{halt}_n, 1/2)$$

$$\geq \max\{\mathcal{E}(\mathcal{V}^{halt}_{2^n}, \tfrac{1}{2}), 2^{2^n}\}$$

$$\geq \ldots \quad 2^{2^{2^n}}$$

$\Rightarrow \nexists$ finite dim. strat achieving val $\frac{1}{2}$

$$\varepsilon(\gamma^{halt}, \tfrac{1}{2}) = \infty$$