6.S979 Lecture 21

No class next week (Thanksgiving break)

Last time: Used PBT to delegate a quantum computation

$$BQP \subseteq MIP^*[\underbrace{\ldots}_{\text{efficient provers}}]$$

Today: Use (fancier) PBT to delegate an MIP protocol

$$NEXP \subseteq MIP^*[q = \log(n),\ a = \mathrm{poly}(n)]$$

$NEXP = MIP[\mathrm{poly}(n), \mathrm{poly}(n)]$

Protocol parameters:

$$MIP[\underset{\substack{\uparrow \\ \text{question length}}}{q}, \underset{\substack{\uparrow \\ \text{answer length}}}{a}]$$

Upper bound on MIP:

$\mathrm{MIP}[\mathrm{poly}(n), \mathrm{poly}(n)]$

$\Rightarrow$ cl. strategy can be described in $\exp(n)$ bits

$\Rightarrow \mathrm{MIP}[\mathrm{poly}(n), \mathrm{poly}(n)] \subseteq \mathrm{NEXP}$

$\mathrm{MIP}[\log(n), \mathrm{poly}(n)] \subseteq \mathrm{NP}$

? $\mathrm{MIP}^*[\log(n), \mathrm{poly}(n)] \supseteq \mathrm{NEXP}$

more magic $\Longrightarrow$ $\mathrm{NEEXP} \subseteq \mathrm{MIP}^*[\mathrm{poly}(n), \mathrm{poly}(n)]$

[N, Wright]

Fancier PBT:

Recall: Verifier can force provers to share $|EPR^{\otimes n}\rangle$, measure in X or Z basis

$q = \text{poly}(n)$

$a = \text{poly}(n)$

One can show: $\exists$ protocol w/ same guarantee (X or Z measurements on $|EPR^{\otimes n}\rangle$)

$q = \log(n)$, $a = \text{poly}(n)$

"quantum low-degree test"

PBT w/ the BLR subtest 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":

$A \quad |EPR^{\otimes n}\rangle \quad B$

$|\psi\rangle$

"X-basis measmt" x

a = the outcome of X-basis meas. of $|EPR^{\otimes n}\rangle$

a' = outcome of any measurement

$$M^{\text{"X-basis"}, x}_{a, a'} = |a_x\rangle\langle a_x| \otimes M^{a_x, x}_{a'}$$

Then $\exists$ G' works for arbitrary q. provers

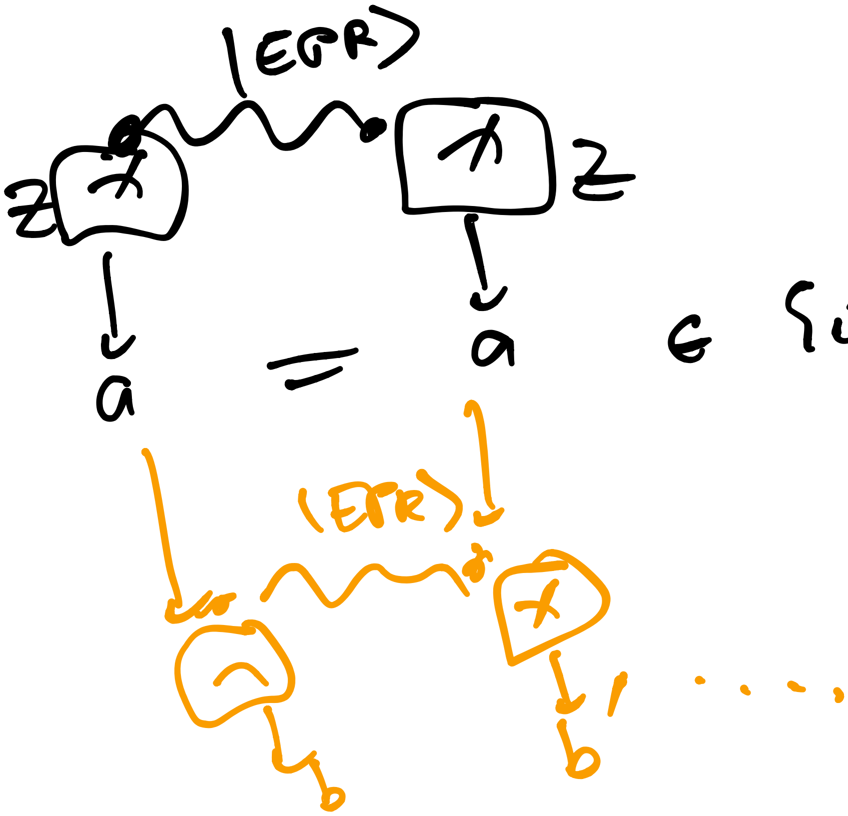
$$G' = \begin{cases} 1/3 & G \\ 1/3 & \text{QLD} \\ 1/3 & \text{consistency} \end{cases}$$

$$G[q, a] \longrightarrow G'[q + \log(n),\ a + \text{poly}(n)]$$

Compression by introspection

Q. key distribution

Randomness expansion

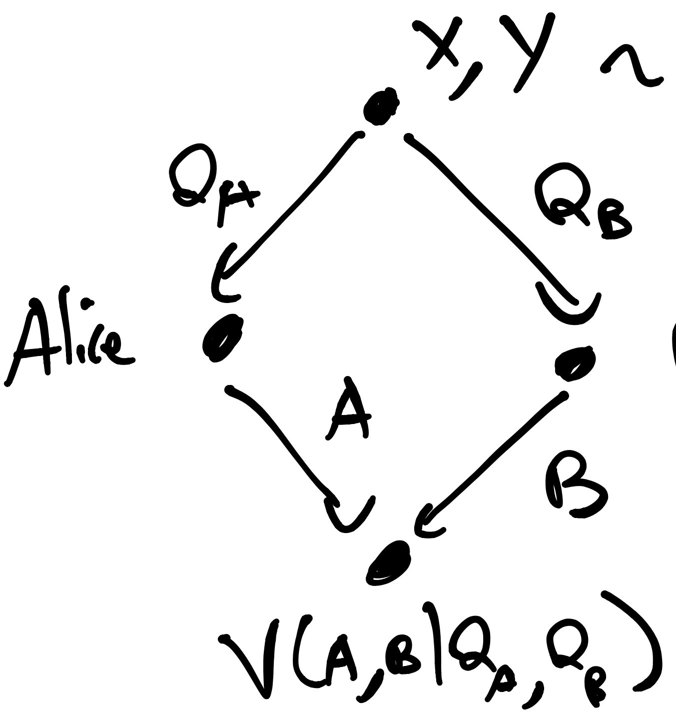


$\in \{0,1\}$

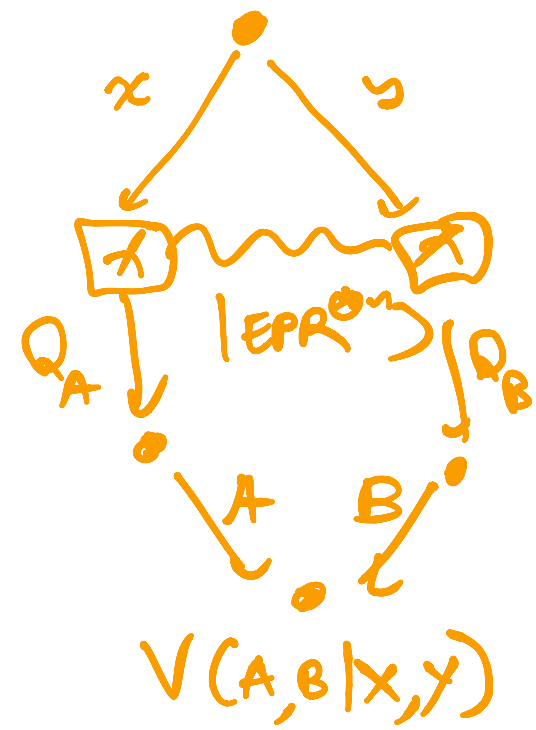
Today: app's this idea to MIP* protocol

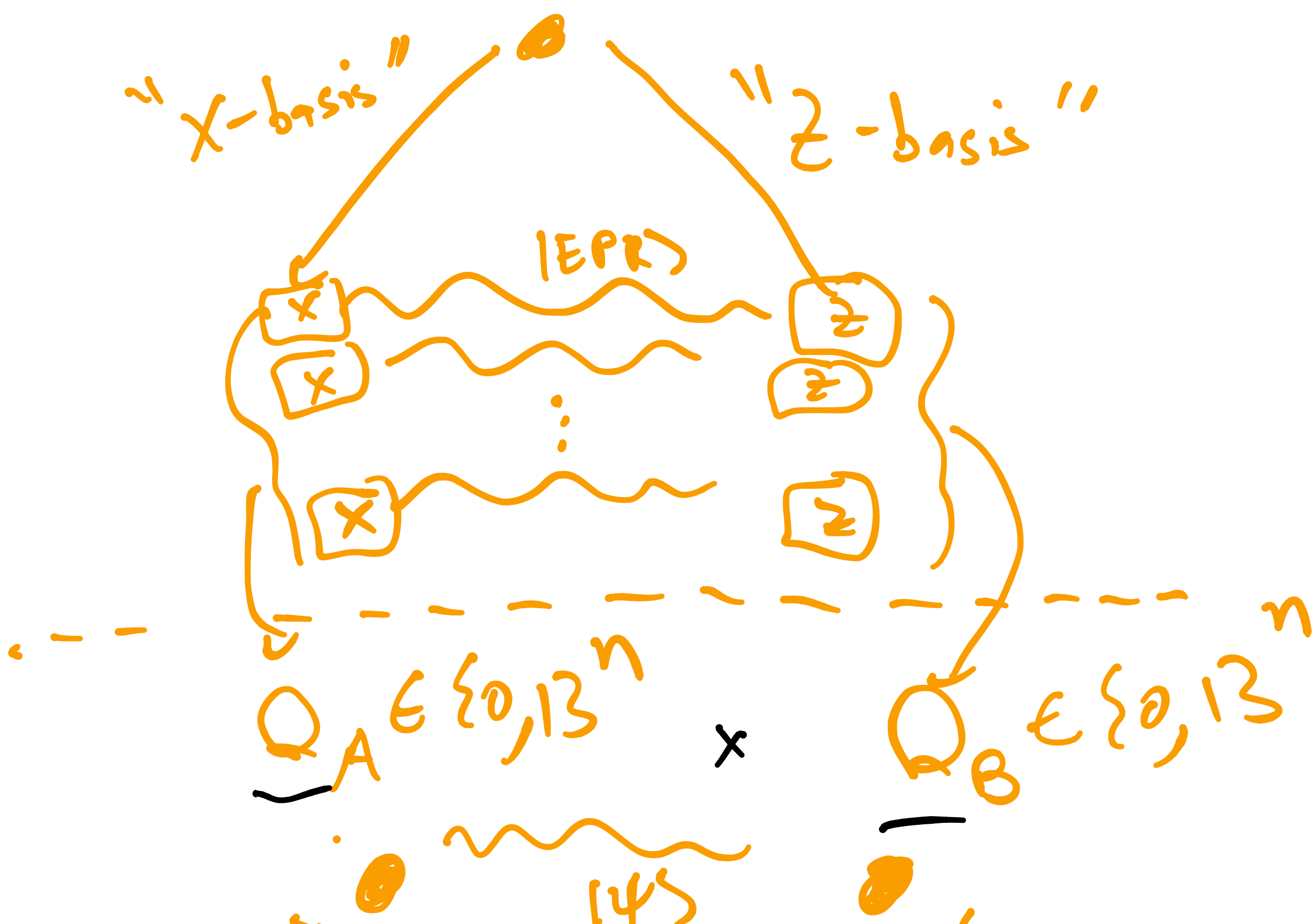
Say $\mathcal{G}$ is an MIP protocol

with $q = \mathrm{poly}(n)$, $a = \mathrm{poly}(n)$



$\Rightarrow$





Original Alice

Original Bob

(Q_A, A) (Q_B, B)

$$V(A, B \mid Q_A, Q_B)$$

$$G[n, a] \longrightarrow G'[1, a+n]$$

only sound against Pauli strategies

$$\xrightarrow{\text{Compiler}} G''[1+\log(n), a+n+\mathrm{polylog}(n)]$$

Potential worry:

After obtains Q_A, Alice could do more measurements on residual q. state to learn something about Q_B

<u>This is impossible</u>: An X-basis measurement of a qubit "destroys" Z-basis information

$$|EPR\rangle = |00\rangle + |11\rangle$$

$\downarrow$ Alice measures in X basis to get $+$

$$|\psi'\rangle = |+\rangle \otimes |+\rangle$$

$\downarrow$ Bob measures to get 1

$$|+\rangle \otimes |1\rangle$$

Suppose G has questions

$$Q_A = u \in \{0,1\}^n$$

$$Q_B = u, v \in \{0,1\}^n$$

$$u \in Z \;\boxed{\hat{x}}\; \bullet \sim |EPR^{\otimes n}\rangle \sim \bullet \;\boxed{\hat{x}}\; Z \to u$$

$$u' \in X \;\boxed{\hat{x}}\; \bullet \sim |EPR^{\otimes n}\rangle \sim \bullet \;\boxed{\hat{x}}\; Z \to v$$

<u>Problem</u>: Alice could have sneakily measured 2^{nd} block of EPRs and learnt v

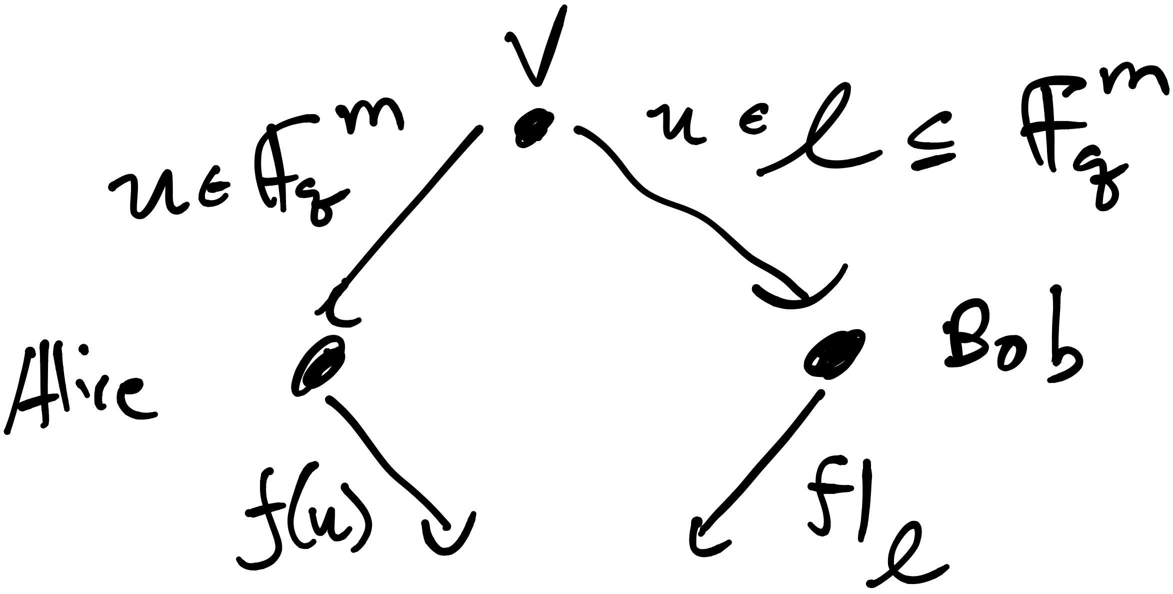
The X-basis outcome u' certifies that Alice didn't peek at v

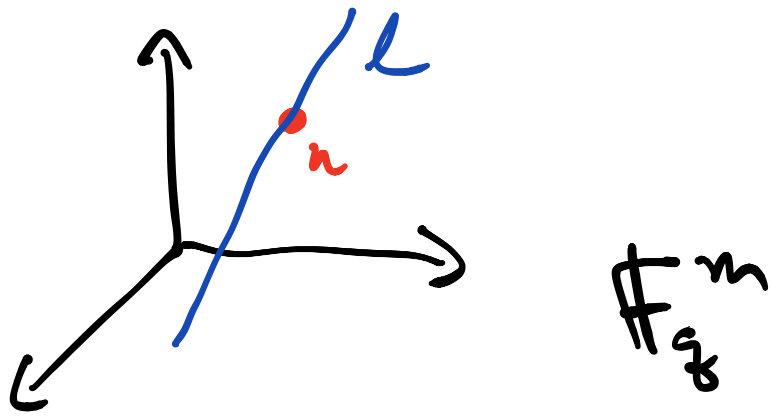
NEXP & the line-point test

MIP = NEXP

coloring

multivar polynomial f on $\mathbb{F}_q^m$





Alice's Q: $u \in \mathbb{F}_q^m$

Bob's Q: $\ell = \{u + \lambda v : \lambda \in \mathbb{F}_q\}$

$\in \mathbb{F}_q^m$

intercept

slope

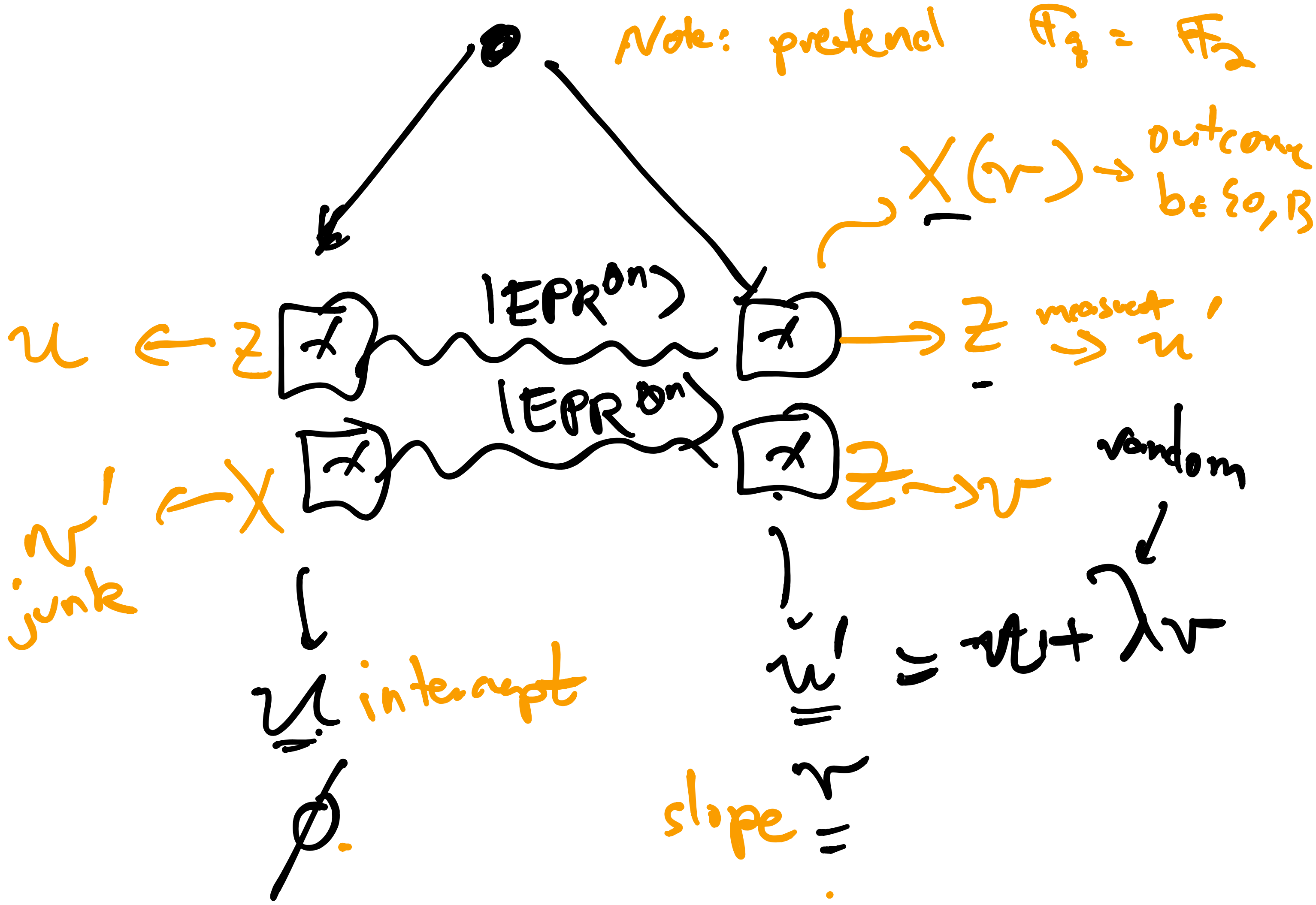
"canonical description" of ℓ

slope v

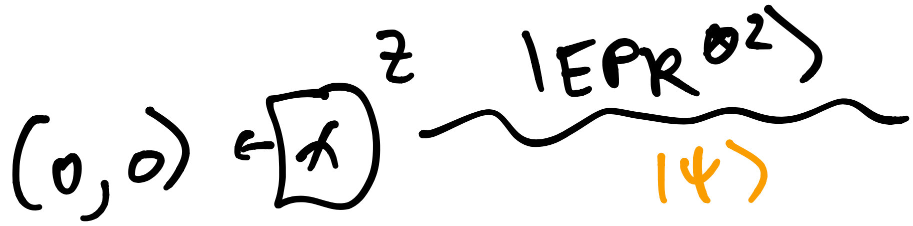
"scrambled intercept" $u \bmod v$

$$u' = u + \lambda v$$

random



Example: $n = 2$, $u, u', v \in \{0,1\}^2$



$$|\psi\rangle = |0,0\rangle_A \; |0,0\rangle_B$$

Bob measures $X(v) = X \otimes X$

eigenstates of $X \otimes X$

$b = +1: \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

$b = -1: \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

$$|\psi_{w,\lambda}\rangle = \frac{1}{\sqrt{2}} \sum_{\lambda} (-1)^{b\cdot\lambda} |w + \lambda v\rangle$$

$$|\psi'\rangle = |00\rangle_A \otimes \frac{1}{\sqrt{2}}(|\underline{00}\rangle \underset{?}{\pm} |\underline{11}\rangle)$$

Pf: (super sketchy):

You know from QLD that X & Z basis measurements are correctly done.

$$Z - \boxed{x} \sim\sim \boxed{x} \to M^{v}_{u',b}$$

supposed to be $X(v)$ then Z

$$-X\ \boxed{x} \sim\sim \boxed{x}\ Z \to v$$

Prove that $[M^{v}_{u',b}, X(v)] \overset{/}{=} 0$

$$a \leftarrow X\ \boxed{x} \sim\sim \boxed{x}\ M^{v}_{u',b}$$

$$b \overset{?}{=} a \cdot v$$

$$\Longrightarrow \quad NEXP \subseteq MIP^{*}[\log(n), \mathrm{poly}(n)]$$

vs.

$$NP = MIP[\log(n), \mathrm{poly}(n)]$$