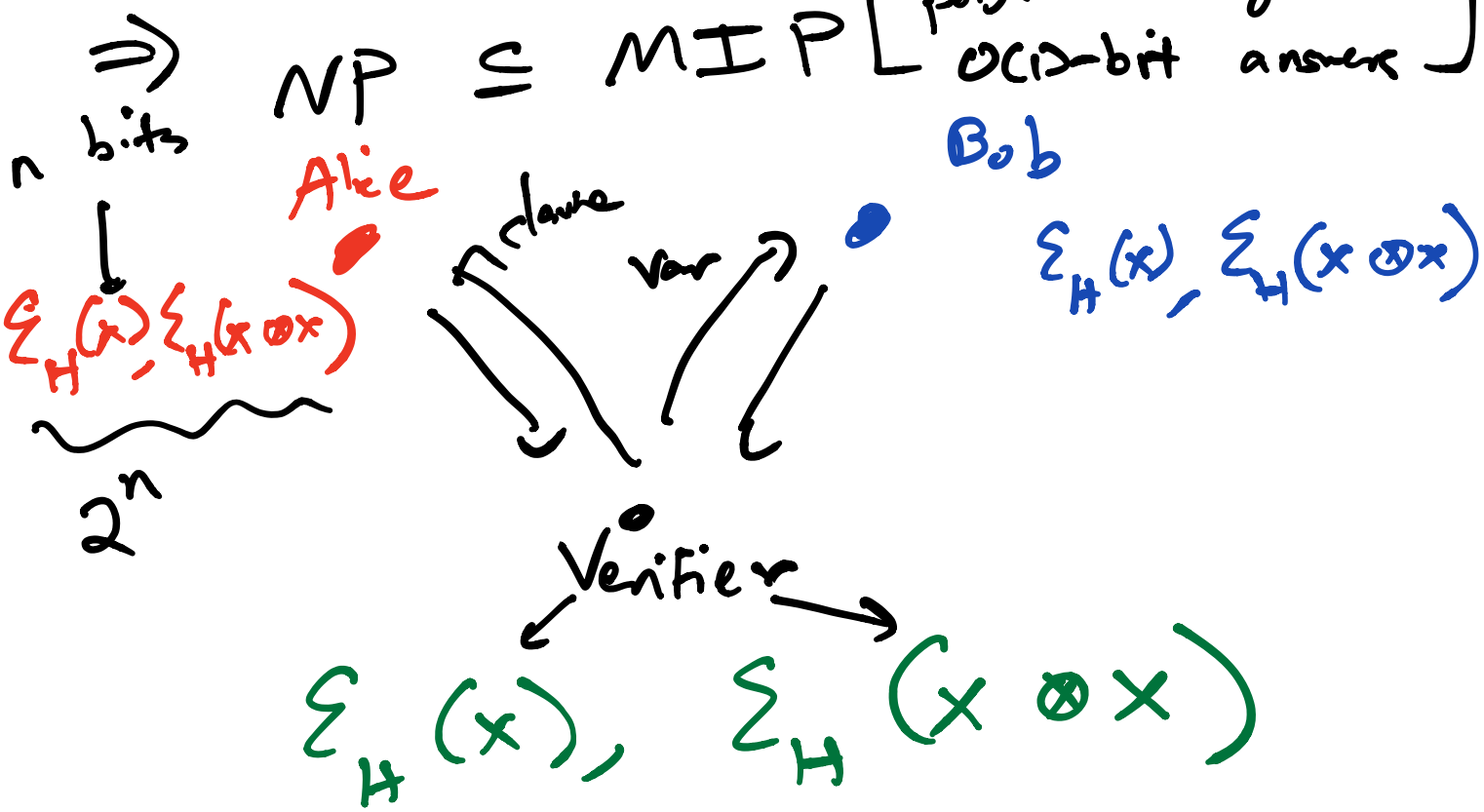
6.5979 Lecture 17

Last time:

Clause Variable Game

+ Hadamard Encoding for quadratic equations ← NP

$\Rightarrow$ $NP \subseteq MIP$ [poly(n)-bit question, O(1)-bit answer]



Recall: $NP \subseteq MIP$ "by default"

- Alice
- Bob is ignored

NP proof → V

You can use the same ideas to show

$$NP = MIP[\log(n)]$$

$$\Rightarrow NEXP = MIP[\text{poly}(n)]$$

Clause variable game

+ a more efficient encoding

"Low degree code" / "Reed Muller code"

$x \longrightarrow \mathcal{E}_{LD}(x)$

x: n bits

$\mathcal{E}_{LD}(x)$: ? $n^{O(\log n)}$ bits

Recall: $\mathcal{E}_H(x)$ = linear function through the values fit of x

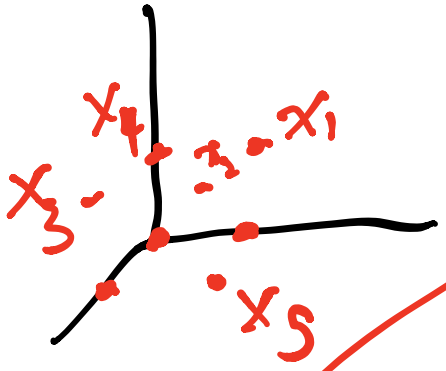
$f(0\ldots01) = x_n$

$f(10\ldots0) = x_1$

$f(01\ldots0) = x_2$

$\vdots$

$\mathcal{E}_{LD}(x)$ = low-degree polynomial fit through values of x



NP = MIP[log(n)]

"PCP theorem"

probabilistically checkable proofs

CV game

for any language in NP, $\exists$ V that takes in proofs Π of length $poly(n) = 2^{\log(n)}$ and decides YES or NO based on O(1) of randomly chosen locations

Technically: the biggest challenge (IMO) is finding a version of BLR test for LD code.

The real goal: Understand

$MIP[C_{ga}]$ or $MIP[C_{ge}]$

$= MIP^*$ $= MIP^{co}$

First goal: $MIP \overset{?}{\subseteq} MIP^*$

(Recall: $MIP^{*\oplus} \subsetneq MIP^{\oplus}$)

An approach:

- Does the Clause-Variable game work for MIP^*?

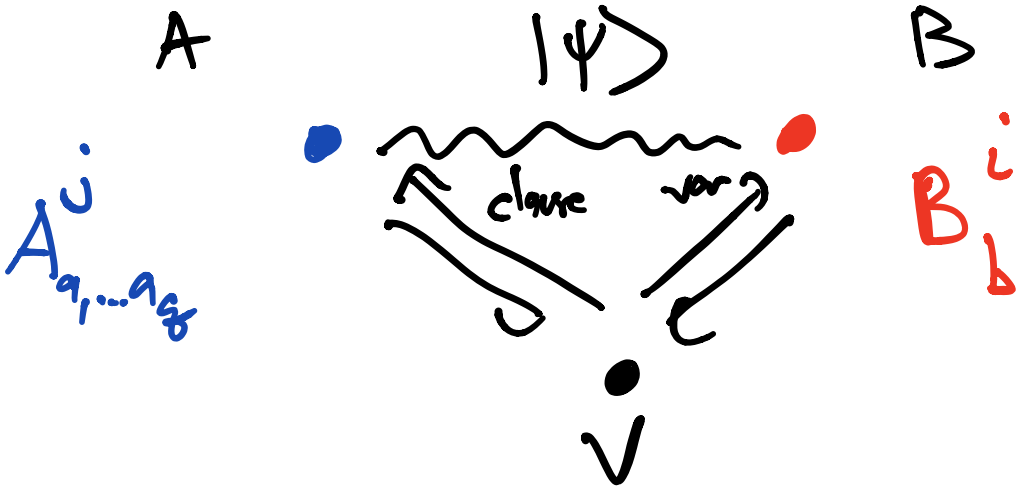
Problem: CV is not sound

Soundness $\quad co(\mathcal{I}) \leq \frac{1}{2} \not\Rightarrow co^*(\mathcal{G}) \leq 1 - \frac{1}{100}$

Ex: Magic Square

$$\omega(\mathbb{D}) = 8/9$$

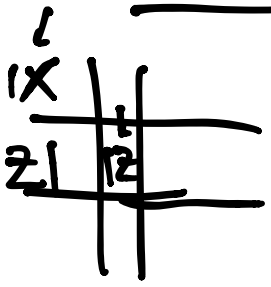
$$\omega^*(G) = 1$$



Assume that $\omega^*(G) \geq 1 - \varepsilon$

Classically: Bob's strat $\Rightarrow$ assignment

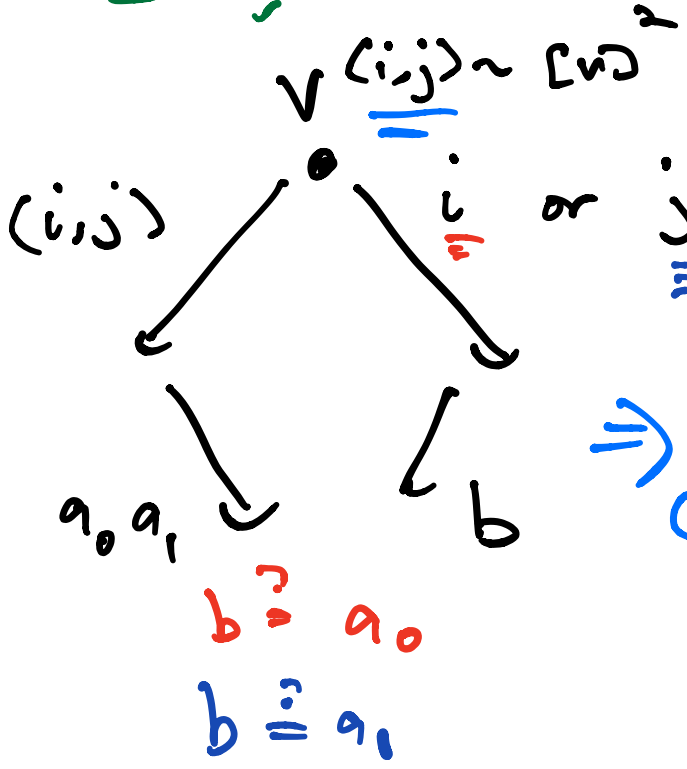
Quantum: $[B^i_b, B^j_b] \neq 0$



Modifications to CV:

1) Just test directly that

$$[B^i, B^j] \approx 0$$



Success in test

$$\Rightarrow \mathop{\mathbb{E}}_{(i,j)} \left\| [B^i B^j] |\psi\rangle \right\|^2 \leq \text{small}$$

Bob's q. strat $\Longrightarrow$ assignment for Φ

$B^n \cdots B^3 B^2 B^1 |\psi\rangle$

$(b_n \cdots b_2 b_1)$ on average should be good assignments for Φ

$\Rightarrow NP \subseteq MIP^*[\log(n) \text{ messages}]$

$c = 1$

$s = 1 - \frac{1}{\text{poly}(n)}$

$NEXP \subseteq MIP^*[\text{poly}(n) \text{ messages}]$

$c = 1$

$s = 1 - \frac{1}{\exp(n)}$

[Ito Kobayashi Matsumoto '09]

Earlier for 3 or more provers

This comes from errors adding up in sequential measurement.

$f(x_1, x_{70}, x_n)$

$B^n \ldots B^{70} \ldots B^3 B^2 B^1 |\psi\rangle$

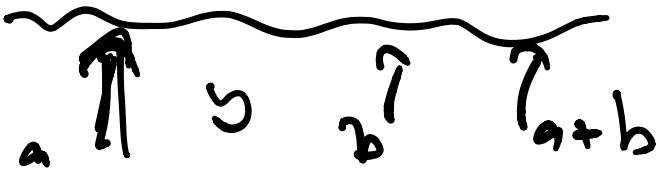
CV game tells you

$B^n B^{70} B^1 |\psi\rangle \rightarrow$ good assignment for f

Attempt #2:

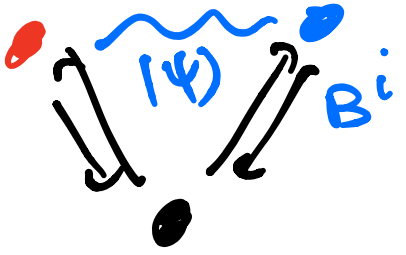
CV + locally testable codes

Recall:



$y \approx \varepsilon_H(x)$

(*) **Ideally:** There is some test s.t.



If $A \nleftrightarrow B$ succeed in test then

$\exists \{M^x\}_x$ ← simultaneously measure all the B^i's

s.t. $B^i_b = \sum_{x:\, \varepsilon_H(x)_i = b} M^x$

i.e., to measure B^i:

- Measure $M \longrightarrow x$
- return $\varepsilon_H(x)_i$

If (*), then if $A \nleftrightarrow B$ succeed in CV + new test

$$\Longrightarrow \exists \{M^x\}_x$$

$$x \sim \langle \psi | M^x | \psi \rangle$$

↑ good assignments to Φ

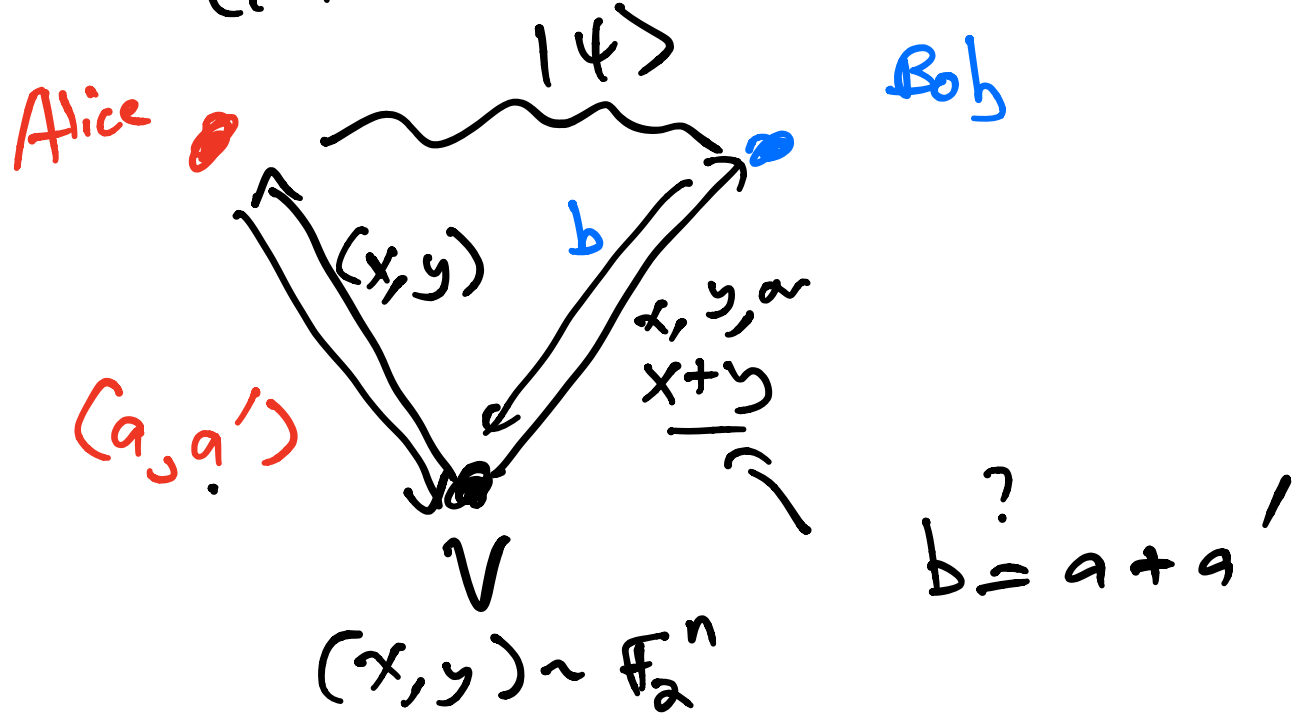
This actually works! ∃ codes for which (*) holds "quantum-sound locally testable code"

(note: nothing to do w/ quantum error correction)

- $\mathcal{E}_H$ works
- A variant of $\mathcal{E}_{2D}$ works ("low individual degree code")
- More??

Thm: $\mathcal{E}_H$ is a quantum sound LTC.

Pf: Use the BLR test (converted to a 2-player game)



Step 1:

From success in test, can show

"commutation subtest" → $A^{x,y}_{a,a'} \otimes I\,|\psi\rangle \approx I \otimes B^{x}_{a} B^{y}_{a'}\,|\psi\rangle$

"BLR" subtest → $A^{x,y}_{a,a'} \otimes I\,|\psi\rangle \approx A^{x,b}_{a,a'} \otimes B^{x+y}_{a+a'}\,|\psi\rangle$

$$\Rightarrow^{(f)} \sum_{a,a'} \mathop{\mathbb{E}}_{x,y} \langle \psi | I \otimes B^x_a B^y_{a'} B^{x+y}_{a+a'} | \psi \rangle \approx 1$$

(Classically: $\Pr[f(x)+f(y)=f(x+y)] \approx 1$)

Step 2:

Define binary observables:

$$B^x = B^x_0 - B^x_1 = \sum_a (-1)^a B^x_a$$

(Classically: ± 1-valued functions)

Define Fourier transform of B:

$$\hat{B}^u = \mathop{\mathbb{E}}_x (-1)^{\langle x,u \rangle} B^x$$

Plancherel formula:

$$\sum_u (\hat{B}^u)^2 = \sum_u \mathop{\mathbb{E}}_{x,y} (-1)^{\langle x+y,u \rangle} B^x B^y$$

Recall: $\sum_u (-1)^{f(u)} = 0$ iff $a \neq 0$

$$= \sum_{x,y} 1[x=5] \cdot 2^n \left(B^x\right)^2$$

$$= \sum_x \left(B^x\right)^2$$

$$\sum_u \left(\hat{B}^u\right)^2 = I$$

$(\dagger) \Rightarrow$ $\sum_u \langle\psi| I \otimes \left(\hat{B}^u\right)^3 |\psi\rangle$

$$\approx 1$$

(Classically: $\sum_u \hat{f}(u)^3 \approx 1$)