Last time: Complexity class IP
example: Graph non-isomorphism

<u>Thm</u> (Fortnow, Karloff, Lund, Nisan; Shamir) $IP = PSPACE$

Believed: $NP \subsetneq PSPACE$

$M\underline{I}P$: multiple provers
Key: Cooperating, non-communicating

Clear: $IP \subseteq MIP$

<u>Thm</u> (Babai, Fortnow, Lund) $MIP = NEXP$
"Police-style interrogations"

Believed: PSPACE $\subsetneq$ NEXP

$\therefore$ IP $\subsetneq$ MIP

two provers
one round

Fact: $\mathrm{MIP} = \mathrm{MIP}(2,1)$

Input: z

Sequence of random bits r, poly in $|z|$.

$\underline{V}(z,r) \rightsquigarrow$ two "questions" x, y.

strings size poly in $|z|$

Provers: Alice & Bob.

x y

Somehow: Respond with z

a b

Verifier "decides" using $\underline{V}(z, r, x, y, a, b)$.

Nonlocal game with k questions and n answers is a pair $G = (\pi, D)$.

where π is a prob. dist. on $[k]\times[k]$ (here $[k]=\{1,\dots,k\}$) and

$D:[k]\times[k]\times[n]\times[n]\to\{0,1\}$ decision predicate

Strategy "Matrix" $p(a,b\mid x,y)\in[0,1]^{k^2n^2}$

= prob Alice responds with a & Bob with b if they were asked x & y.

Above: deterministic strategies

$A:[k]\to[n]$

$B:[k]\to[n]$

$p(A(x),B(y)\mid x,y)=1$

$C_{det}\subseteq[0,1]^{k^2n^2}$ set of deterministic strategies

If p is a strategy, define

$$\mathrm{val}(G,p):=\sum_{(x,y)\in[k]^2}\pi(x,y)\sum_{(a,b)\in[n]^2}D(x,y,a,b)\,p(a,b\mid x,y)$$

expected value of winning $\mathcal{G}$ if they play according to strategy p.

$$\mathrm{val}(\mathcal{G}) := \sup_{p \in C_{det}(k,n)} \mathrm{val}(\mathcal{G}, p)$$

<u>classical value of $\mathcal{G}$</u>

Rephrase MIP: L belongs to MIP iff there is an "effizient mapping"

$$z \mapsto \mathcal{G}_z \text{ so that:}$$

- If $z \in L$, then $\mathrm{val}(\mathcal{G}_z) \geq \frac{2}{3}$
- If $z \notin L$, then $\mathrm{val}(\mathcal{G}_z) \leq \frac{1}{3}$.

MIP*: same using $\mathrm{val}^*(\mathcal{G}) = \sup$

quantum strategies

Quantum Theory

Axioms:

Physical system $\rightsquigarrow$ Hilbert space H

State of the system $\xi \in H$, $\|\xi\| = 1$.

Evolves linearly according to some PDE until it is "measured"

Us: Measurements w/ finitely many outcomes

e.g. spin of electron : "up" or "down"

n outcomes $\rightsquigarrow$ n bounded operators $M_1, \ldots, M_n$ on H

Born rule If $\xi \in H$ is the state of the system upon measurement, then the prob. that measurement $i \in \{1, \ldots, n\}$ occurs is $\|M_i(\xi)\|^2$. In this case, the state instantaneously (& discontinuously) collapses to $\dfrac{M_i(\xi)}{\|M_i(\xi)\|}$.

$$1 = \sum_{i=1}^{n} \|M_i(\xi)\|^2 = \sum_{i=1}^{n} \langle M_i^* M_i(\xi), \xi \rangle$$

True $\forall \xi, \|\xi\| = 1 \Rightarrow \boxed{\sum_{i=1}^{n} M_i^* M_i = I}$

Only interested in probabilities:
replace M_i's by positive operators $A_1, \ldots, A_n$, $\sum_{i=1}^{n} A_i = I$.

Prob of i^{th} outcome is $\langle A_i(\xi), \xi \rangle$.
POVM: positive operator valued measure
If each A_i is actually a projection, then they are mutually orthogonal, so <u>PVM</u>
$A_i A_j = A_j A_i = 0$ if $i \neq j$.

example spin of an electron

"up" or "down" (fixing, say, vertical axis)

Hilbert space $H = \mathbb{C}^2$

e_1, e_2 usual basis vectors

"up" "down"

$|up\rangle$ & $|down\rangle$

$|0\rangle$ & $|1\rangle$

general state: $\psi = \alpha_1 e_1 + \alpha_2 e_2$, $\alpha_1, \alpha_2 \in \mathbb{C}$

$$\|\psi\|^2 = 1 \Rightarrow |\alpha_1|^2 + |\alpha_2|^2 = 1.$$

Measurement: PVM $A_1 =$ proj. onto e_1

$A_2 =$ proj. onto e_2.

Prob of up $= |\alpha_1|^2$

Prob of down $= |\alpha_2|^2$

"superposition"

Hilbert spaces H_A & H_B for two physical systems

Composite system: $H_A \otimes H_B$

Elements of $H_A \otimes H_B$ are not simply of the form $v \otimes w$ $\rightsquigarrow$ quantum entanglement

$\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ two electrons

$\psi_{EPR} = \frac{1}{\sqrt{2}}(e_1 \otimes e_1 + e_2 \otimes e_2) \in \mathbb{C}^2 \otimes \mathbb{C}^2$

Einstein, Podolsky, & Rosen

John Bell: Experiment test for winner

Winner: Quantum

"hidden variable"

Local Strategies: (Ω, μ) prob. space

For $\omega \in \Omega$, $A_\omega : [k] \to [n]$

$B_\omega : [k] \to [n]$

$$p(a,b|x,y) := \mu(\{\omega \in \Omega : A_\omega(x) = a, \ B_\omega(y) = b\})$$

$C_{loc}(k,n) \subseteq [0,1]^{k^2n^2}$ convex

convex hull of $C_{det}(k,n)$.

$val(G) = \sup_{p \in C_{loc}(k,n)} val(G,p)$

Alice Bob

Quantum strategies: H_A & H_B

finite-dimensional!

on HA

For each $x \in [k]$, POVM $(A^x_a)_{a \in [n]}$. $\sum_{a \in [n]} A^x_a = I$ $\forall x$.

" " $y \in [k]$ POVM $(B^y_b)_{b \in [n]}$.

$\psi \in H_A \otimes H_B$. state

$p(a,b|x,y) = \langle (A^x_a \otimes B^y_b)\psi, \psi \rangle$

$C_q(k,n)$ = set of such quantum strategies

closed convex

convex $\boxed{\text{closed?}}$

Check: $C_{loc}(k,n) \subseteq C_q(k,n)$

$val^*(G) = \sup_{p \in C_q(k,n)} val(G,p)$

entangled value of G

$$\mathrm{val}(\mathcal{G}) \leq \mathrm{val}^*(\mathcal{G}).$$

Bell's Thm recast (CHSH): $\exists \mathcal{G}$
$$\mathrm{val}(\mathcal{G}) < \mathrm{val}^*(\mathcal{G}).$$

$\mathcal{G}_{CHSH}$: $k=n=2$.

π: uniform dist. on $[2]\times[2]$.

- If $x=1$ or $y=1$, then win iff same answer.
- If $x=2$ and $y=2$, then win iff diff. answers.

Check: $\mathrm{val}(\mathcal{G}_{CHSH}) = \frac{3}{4}$.

$\exists p \in C_q(2,2)$ s.t. $\mathrm{val}(\mathcal{G}_{CHSH}, p) = \underbrace{\cos^2\left(\frac{\pi}{8}\right)}_{\mathrm{val}^*(\mathcal{G})}$
$$\approx 0.85$$
$$> \frac{3}{4}$$

Based on Ψ_{EPR}.

$\text{MIP} = \text{NEXP}.$

$$\begin{tikzcd}
& & \neg\,\text{Tsirelson} \arrow[d, Rightarrow] \\
\boxed{\text{MIP}^* = \text{RE}} \arrow[urr, Rightarrow] \arrow[rr, Rightarrow] \arrow[d, Rightarrow, "\boxed{\text{Model theory}}"] & & \neg\,\text{QWEP} \arrow[dll, Rightarrow, bend left] \\
\neg\,\text{CEP} & &
\end{tikzcd}$$