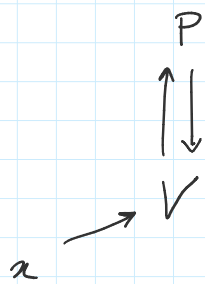
Lecture 8 – Multiprover interactive proof systems

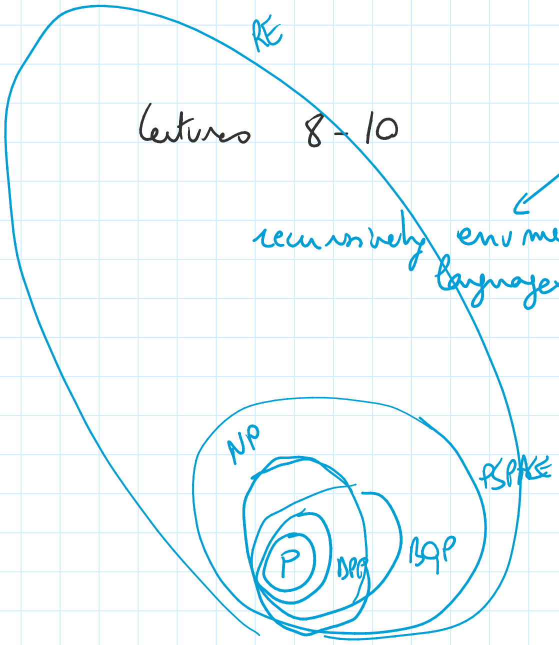
Tuesday, November 17, 2020 9:48 AM

Lectures 4-7 $BQP \subseteq IP[BQP]$

Prover cannot break LWE assumption



(BPP)

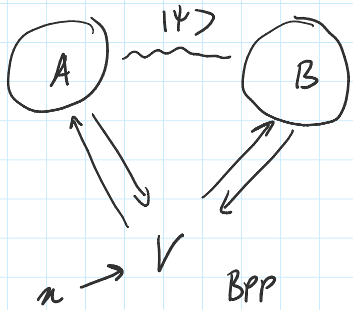


Lectures 8-10 $RE = MIP^*$ $(= MIP[ALL])$

recursively enumerable languages

multiple provers

cheating prover has arbitrary comp power.



Def: A promise language $L = (L_{yes}, L_{no})$ is in MIP^* iff $\exists$ poly-time Turing machine $M : 1^n \to V_n$, description of a BPP verifier st the following holds:

(i) Completeness: $\forall x \in L_{yes}$, $\exists$ quantum provers (A,B) st $V_{|x|}$ accepts x and (A,B) wp $\geq 2/3$

(ii) Soundness: $\forall x \in L_{no}$, $\forall$ quantum provers (A,B) $V_{|x|}$ accepts x and (A,B) wp $\leq 1/3$.

A – Classical multiprover interactive proofs

MIP

Graph coloring

$x = (1^n, C)$ st C is a classical circuit

$C : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$x = (1^n, C)$ st C is a classical circuit
$C : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

To x, associate graph $G_x = (V_x, E_x)$
$V_x = \{0,1\}^n$
$(i,j) \in E_x$ iff $C(i,j) = 1$

Thm Fact L: $L_{yes} = \{ x = (1^n, C)$ st G_x is 3-COL$\}$
$L_{no} = \{ x = (1^n, C)$ st G_x is not 3col$\}$.

L is NEXP-complete.

MIP for L:
Verifier: 1) Parse its input $x = (1^n, C)$
2) Select $i, j \leftarrow_R \{0,1\}^n$
Send i to A, j to B.

3) A returns $a \in \{0,1,2\}$
B returns $b \in \{0,1,2\}$

4) Accept iff either (i) $i = j$ and $a = b$
(ii) $C(i,j) = 1$ and $a \neq b$
(iii) $C(i,j) = 0$

Classical strategies: $f_A, f_B : \{0,1\}^n \to \{0,1,2\}$.

Def $\omega(V$ on input $x)$ = maximum success prob of classical provers in protocol.

Claim • if G_x is 3col then $\omega(V_x) = 1$
• if G_x is not 3col then $\omega(V_x) \leq 1 - 2^{-\Omega(n)}$

Thm • Can show that $L \in$ MIP
$\Rightarrow$ NEXP $\subseteq$ MIP

• MIP $\subseteq$ NEXP

MIP = NEXP

prove by enumerating over all strategies (f_A, f_B)

B - quantum MIP^*

Provers : $(f_A, f_B) \longleftrightarrow$ (local q. operations on $|\psi\rangle \in H_A \otimes H_B$)

larger class of strategies

$w^*(V_x) \geq w(V_x)$

supremum over quantum strat

supremum over class strat

(i) Complexity-theoretic intuition:
provers can do more $\rightarrow$ MIP^* smaller than MIP

(ii) Optimization intuition:
more complicated class of strategies $\rightarrow$ $w^*(V_x)$ harder to compute

$\rightarrow$ upper bound $MIP^* \overset{?}{\notin} NEXP$

Focus on $MIP^*(2,1)$

two provers

1 round of interaction

C - Nonlocal games

Def A nonlocal game is $G = (\pi, R)$
where π is a dist on $\underbrace{X}_{} \times \underbrace{Y}_{}$
finite q. set

R: decision predicate
$R: X \times Y \times \underbrace{A \times B}_{\text{finite answer set}} \rightarrow \{0,1\}$

"$R(a,b|x,y) = 1$ iff (a,b) are valid answers to (x,y)"

A strategy S for G is $G = \{p(a,b|x,y)\}_{x,y \in X \times Y}$
where $p(\cdot,\cdot|x,y)$ is a dist on $A \times B$.

Success prob $w(G;S) = \sum_{x,y} \pi(x,y) \sum_{a,b} p(a,b|x,y) R(a,b|x,y)$.

Classes of strategies:

- $S_{clas} = \{ p(a,b|x,y) = \int_\lambda P_A(a|x,\lambda)\, P_B(b|y,\lambda)\, d\lambda \}$.

- $S_{quant} = \{ p(a,b|x,y) = \langle\psi| A_a^x \otimes B_b^y |\psi\rangle$ where:

  $|\psi\rangle \in H_A \otimes H_B$, H_A, H_B f.d. Hilbert spaces

  $\mathbb{C}^k \quad \mathbb{C}^k$

  $\forall x$, $\{A_a^x\}_a$ POVM on H_A

  $\forall y$, $\{B_b^y\}$ POVM on H_B.

$\tilde{A}_a^x \in \mathbb{C}^{k\times k}$

$\hat{A}_a^x = (\tilde{A}_a^x)^* \tilde{A}_a^x \geq 0$

$\hat{A}^x = \sum_a \hat{A}_a^x$

$A_a^x = (\hat{A}^x)^{-1/2} \hat{A}_a^x (\hat{A}^x)^{-1/2}$

$$w^*(G) = \sup_{S \in S_{quant}} w(G;S)$$

Complexity of MIP* is "same" as complexity $G \mapsto w^*(G)$

V_n represented by a circuit — G represented explicitly by π, R

poly size $\longleftrightarrow$ exp size.

Lemma $MIP^*_{(2,1)} \subseteq RE$

Pf: To show: Any $L \in MIP^*(2,1)$ is st $L \in RE$

$\Leftrightarrow$ $\exists$ TM M st:

$\forall x \in L_{yes}$, M halts with "YES"

$\forall x \in L_{no}$, M does not halt with "YES"

We know that $\forall x$, $\exists$ nonlocal game G_x (computable from x)

st $x \in L_{yes} \Rightarrow w^*(G_x) \geq 2/3$

$x \in L_{no} \Rightarrow w^*(G_x) \leq 1/3$.

$$\boxed{\begin{array}{l} \text{Algorithm } A: \ (1)\ \text{Compute } G_x \\ (2)\ \text{compute } v_1 \leq v_2 \leq \cdots \leq v_k \leq \cdots \\ \quad \text{where } v_k \text{ is supremum of } w^*(G_x, S) \\ \quad \text{for all q. strategies } S \text{ in an } (1/k)\text{-net} \\ \quad \text{of strategies in dim} \leq k. \\ (3)\ \text{if } v_k > 1/2 \text{ then } A \text{ halts with "YES"} \end{array}}$$

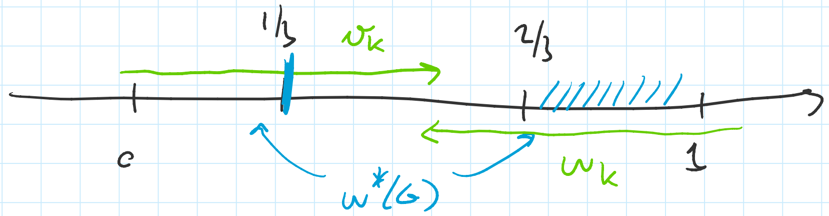
of strategies in dim $\le k$.

(3) if $v_k > 1/2$ then A halts with "YES"

By definition, $\lim_{k \to \infty} v_k = w^*(G_x)$

- If $w^*(G_x) \geq \frac{2}{3}$, $\exists\, k$ st $v_k > \frac{1}{2}$. Then A halts with "YES"
- If $w^*(G_x) \leq \frac{1}{3}$, $\forall k$ $v_k \leq 1/3$ so A never halts.

This shows that $L \in RE$.



To get an actual alg we need

Alg B: $w_1 \geq w_2 \geq \cdots \geq w_k \to w^*(G)$

Upper bounds on $w^*(G)$.

$$w^*(G) = \sup_{\substack{|\psi\rangle \in H_A \otimes H_B \\ A^x_a,\, B^y_b}} \sum_{xyab} \pi(x,y)\, R(a,b|x,y)\, \boxed{\langle \psi | A^x_a \otimes B^y_b | \psi \rangle}$$

$$\leq \sup_{|u^x_a\rangle, |v^y_b\rangle \in H \text{ "} = H_A \otimes H_B \text{"}} \sum_{xyab} \pi(x,y)\, R(a,b|x,y)\, \langle u^x_a | v^y_b \rangle$$

$$\text{st} \begin{cases} \sum_a \| |u^x_a\rangle \|^2 \leq 1 & \forall x \\ \sum_b \| |v^y_b\rangle \|^2 \leq 1 & \forall y \end{cases}$$

$|u^x_a\rangle = A^x_a \otimes \mathbb{I} |\psi\rangle$
$|v^y_b\rangle = \mathbb{I} \otimes B^y_b |\psi\rangle$

$n = |X| = |Y|$
$\ell = |A| = |B|$.

$$w_1 = \sup_{|u^x_a\rangle, |v^y_b\rangle \in \mathbb{C}^{2n\ell}}$$

same norm conditions

semi-definite program

$$= \sup_{\Gamma \in \mathbb{C}^{2n\ell \times 2n\ell}} \sum_{xyab} \pi(x,y)\, R(a,b|x,y)\, \Gamma_{xa,yb}$$

st $\Gamma \succeq 0$

$$\Gamma = \begin{array}{c|cc} & u^x_a & v^y_b \\ \hline u^x_a & \Gamma_{xa,xa} & \Gamma_{xa,yb} \\ v^y_b & \Gamma_{yb,xa} & \Gamma_{yb,yb} \end{array}$$

program

$$\text{st} \quad \Gamma \geq 0 \qquad \Gamma = \begin{array}{c} \\ v_b^y \end{array} \begin{bmatrix} \Gamma_{xa,xa} & \Gamma_{xa,yb} \\ \Gamma_{yb,xa} & \Gamma_{yb,yb} \end{bmatrix}$$

$$\sum_a \Gamma_{xa,xa} \leq 1 \quad \forall x$$

$$\sum_b \Gamma_{yb,yb} \leq 1 \quad \forall y.$$

FACT

- $\omega^*(G) \leq W_1$ (by definition)
- w_1 can be computed in time $\mathrm{poly}(|G|)$.
- There are G st $\omega^*(G) \ll w_1$

Define $$w_k = \sup_{\Gamma^{(k)} \geq 0} \sum_{xyab} \pi(x,y) R(a,b|x,y)\, \Gamma^{(k)}_{xy,ab}$$

$\Gamma^{(k)} \in \mathbb{C}^{\binom{2n\ell}{k} \times \binom{2n\ell}{k}}$

$\Gamma^{(k)}$ is indexed by sequences $m_1 = (x_1,a_1)(x_2,a_2),\dots,(x_k,a_k)$

$\Gamma^{(k)}_{xayb,\,yb} = \Gamma^{(k)}_{xa,yb}$

$u_a^x = A_a^x \otimes \mathbb{I}|\psi\rangle \qquad \boxed{v_b^y = \mathbb{I} \otimes B_b^y |\psi\rangle}$

$\boxed{u_{ab}^{xy} = A_a^x \otimes B_b^y |\psi\rangle}$

$u_{aba'}^{xyx'} = A_a^x A_{a'}^{x'} \otimes B_b^y |\psi\rangle$

$\langle u_{ab}^{xy} | v_b^y \rangle = \langle u_a^x | v_b^y \rangle$

$\left((B_b^y)^2 = B_b^y \right).$

Then,

- $w_1 \geq w_2 \geq \dots \geq w_k \geq \dots \geq \omega^*(G)$
- w_k can be computed in time $|G|^{O(k)}$

Th (NPA '08) $$w_k \to w_{com}(G)$$

where $$w_{com}(G) = \sup_{\substack{|\psi\rangle \in \mathcal{H} \text{ (separable)} \\ A_a^x,\, B_b^y \text{ POVM on } \mathcal{H} \\ \forall xyab \ [A_a^x, B_b^y] = 0}} \sum_{xyab} \pi(x,y) R(a,b|x,y) \langle \psi | A_a^x B_b^y | \psi \rangle$$

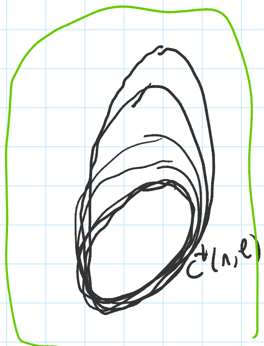
Pf: GNS construction.

Recap : $\quad v_1 \leq \cdots \leq v_k \leq \cdots \boxed{w^*(G) \leq w_{com}(G)} \cdots \leq w_k \leq \cdots \leq w_1$

Algorithm A $\qquad\qquad$ Algorithm B

Corollary of $MIP^* = RE$: $\exists G$ st $w^*(G) \neq w_{com}(G)$.

Tsirelson :



$\subset \mathbb{R}^{(n\ell)\times(n\ell)}$

$$\to C^*(n,\ell) = \left\{ \left(\langle\psi| A_a^x \otimes B_b^y |\psi\rangle\right)_{xyab} : \begin{array}{l} |\psi\rangle \in H_A \otimes H_B \\ A_a^x, B_b^y \text{ POVM} \end{array} \right\}$$

separate

$\cap$

$$C_{com}(n,\ell) = \left\{ \left(\langle\psi| A_a^x B_b^y |\psi\rangle\right)_{xyab} : \begin{array}{l} |\psi\rangle \in H \\ A_a^x, B_b^y \text{ POVM on } H \\ [A_a^x, B_b^y] = 0 \end{array} \right\}.$$

$w^*(G) \neq w_{com}(G)$

Tsirelson : Is $\overline{C^*(n,\ell)} \neq C_{com}(n,\ell)$? NO.

Slofstra '18 : The set $C^*(n,\ell)$ is not closed

Fact $\quad$ (1) If we restrict all spaces to be f.d. then $C^*(n,\ell) = C_{com}(n,\ell)$ $\forall n,\ell$

(2) $\displaystyle w^*(G) = \sup_{\substack{|\psi\rangle \in H_A \otimes H_B \\ H_A, H_B \text{ f.d.}}} \text{———} = \sup_{\substack{|\psi\rangle \in H_A \otimes H_B \\ H_A, H_B \text{ infinite dim}}} \text{———}$

E - Connes Embedding Problem (CEP)

Connes '1976 $\quad$ " every type II_1 von Neumann algebra ought to embed into R "

Kirchberg '93 $\quad$ QWEP conjecture

$$C^*(\mathbb{F}_2) \otimes_{min} C^*(\mathbb{F}_2) = C^*(\mathbb{F}_2) \otimes_{max} C^*(\mathbb{F}_2) \, ?$$

QWEP $\iff$ CEP

Fritz, JNP, Ozawa : QWEP $\iff$ Tsirelson's pb.

Corollary 2 $\quad MIP^{*} = RE \Rightarrow$ CEP is false

$\Rightarrow \exists$ vN algebra that is "not hyperfinite"