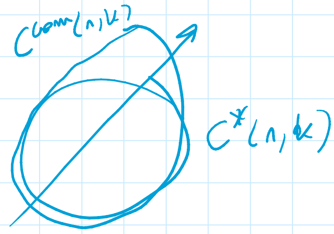
Lecture 9 - Compression of nonlocal games

Tuesday, November 24, 2020 9:59 AM



$MIP = NEXP$ $\rightarrow$ $\boxed{MIP^*_{(2,1)} = RE}$ ($\subseteq$)

$L \in MIP^*$ if $\exists$ poly time TM $V: 1^n \rightarrow$ "verifier" V_n
st V_n is poly time verifier st

(i) $\forall x,\ x \in L \Rightarrow \exists$ q. provers (A,B) st
$V_{|x|}(x)$ accept (A,B) wp $\geq \frac{2}{3}$

(ii) $\forall x,\ x \notin L \Rightarrow \forall$ q. provers (A,B)
$V_{|x|}(x)$ accepts (A,B) wp $\leq \frac{1}{3}$.

$L \in RE$ if $\exists$ TM M st $\forall x$
(i) $x \in L \Rightarrow M(x)$ halts with "YES"
(ii) $x \notin L \Rightarrow M(x)$ either does not halt
or halts with "NO"

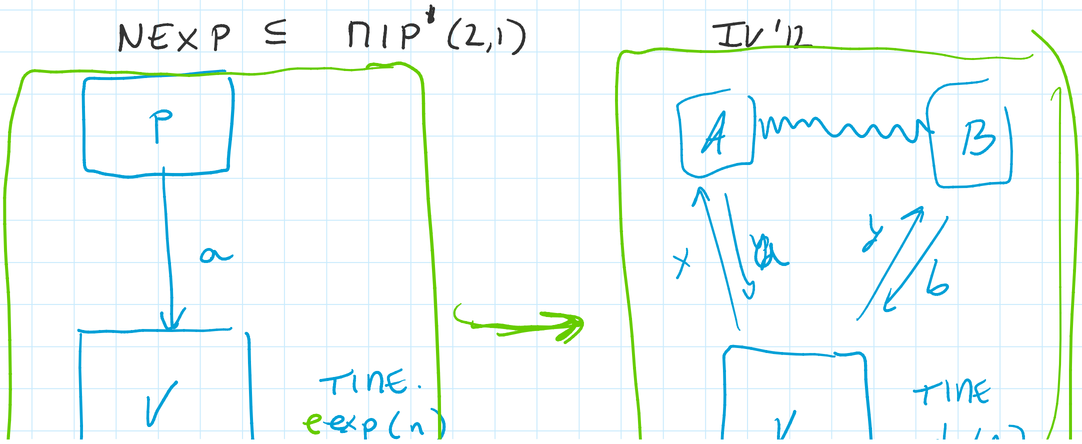
$MIP^*(2,1)$: $\quad V_n(x) \leftrightarrow G_n(x) = (\pi, R)$

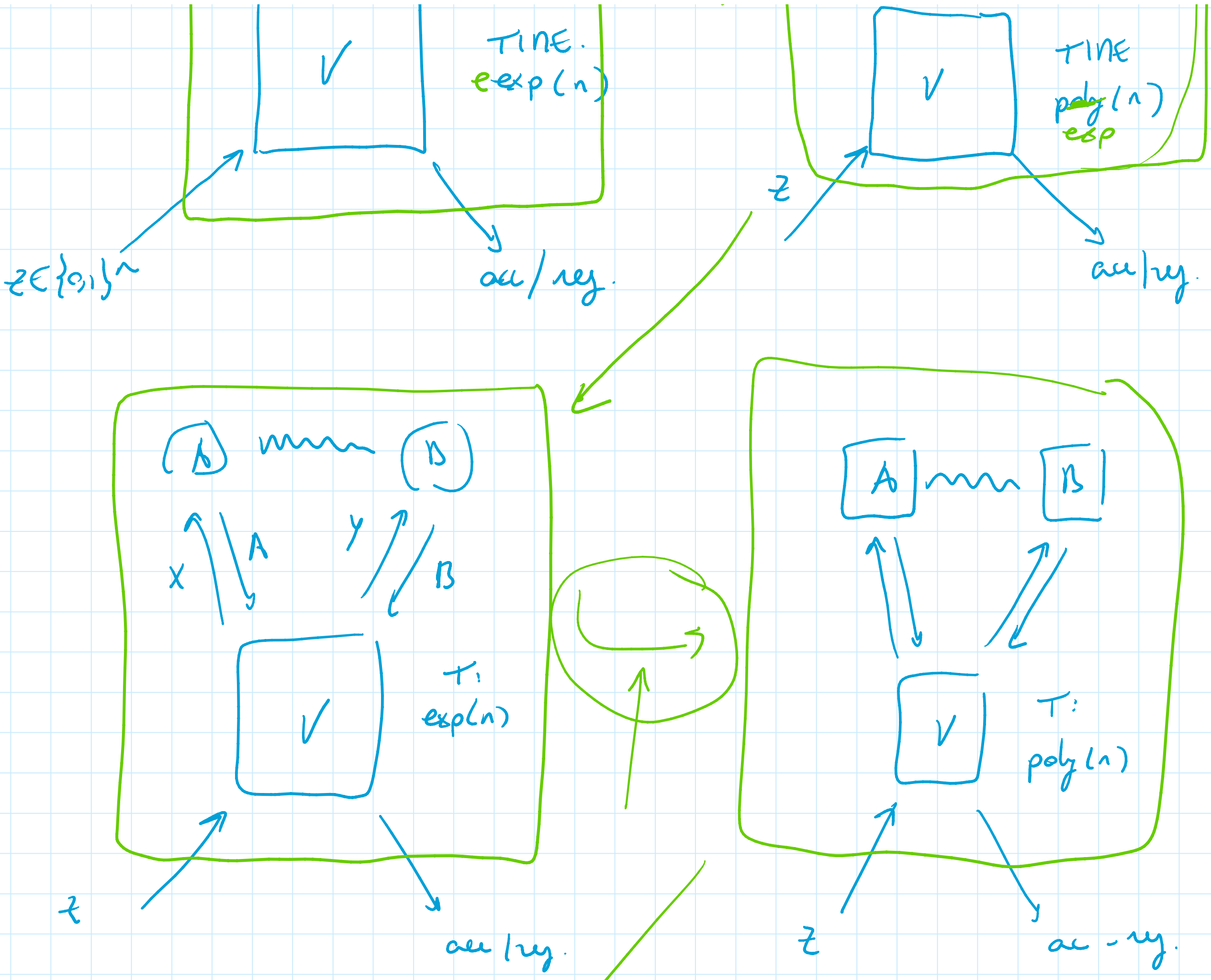
$$\omega^*(G_n(x)) = \sup_{|\psi\rangle,\ A^x_a,\ B^y_b} \underbrace{\sum_{x,y,a,b} \pi(x,y)\, R(a,b|x,y) \cdot \boxed{\langle \psi | A^x_a \otimes B^y_b | \psi \rangle}_{ab}^{xy}}_{\text{linear function on } C^*}$$

$$C^* = \{ (\langle \psi | A^x_a \otimes B^y_b | \psi \rangle)_{abxy} \} \subseteq \mathbb{R}^{n^2 k^2}$$

$NEXP \subseteq MIP^*(2,1)$ IV'12

NEEXP





Thm: $NEEXP \le MIP^*(2,1)$ [NW'18]

Def Halting problem: $L_{HALT} = \{ x \in \{0,1\}^* \text{ st }$

$x = \overline{M}$ st M halts when executed on an empty input tape $\}$.

desc of Turing Machine M

Lemma L_{HALT} is undecidable

Suppose not. Let A be a TM st

$x \in L_{HALT} \Rightarrow A(x)$ halts with "YES"

$x \notin L_{HALT} \Rightarrow A(x)$ halts with "NO"

Define a new TM B st given input $x = \overline{M}$ does the following:

(i) B runs A on x.

If A says "YES" then B enters an ∞ loop

If A says "NO" then B halts with "YES".

Q: what does B return on input $x = \overline{B}$?

CCL: no such A exists.

In fact, L_{HALT} is complete for RE.

Goal Design a computable map

$\mathcal{F} : \overline{M} \longmapsto G_M = (\pi_M, R_M)$ game

st if M halts then $\omega^*(G_M) \geq 1$

M does not halt —— $\leq \frac{1}{2}$.

open.

$coRE \overset{?}{=} MIP^{com}(2,1) \subseteq coRE$ Alg B.

This implies $RE \leq MIP^*(2,1) \subseteq RE$ Alg A.

Compression:

Def • A normal form (NF) verifier is a polytime TM $V: 1^n \longrightarrow R_n$ st $\forall n$, R_n is a class. circuit $: (\{0,1\}^n)^4 \longrightarrow \{0,1\}$

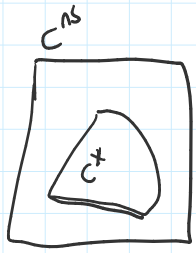
• For integer $\lambda \geq 1$, we say that V is λ-bounded if $\forall n \geq 1$, $TIME(R_n) \leq (\lambda n)^\lambda$

Def: Given game $G = (\pi, R)$ and $p \in [0,1]$ define $\mathcal{E}(G,p)$ = smallest $d \geq 1$ st $\exists$ strategy S for G st $\omega(G;S) \geq p$ and $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$.

ex: If $\omega_{class}(G) = 1$
then $\mathcal{E}(G,p) = 1$ $\quad \forall\, p \in [0,1]$

. If $\omega^*(G) < 1$
then $\mathcal{E}(G,1) = \infty$

. ~~ex~~ $\mathcal{E}(MS, 1) = 4$.



Claim: $\exists$ polynomial time TM $\quad$ COMPR : $(\overline{V}, \lambda) \mapsto \overline{V^{COMPR}}$ s.t.

(a) Always, V^{COMPR} is NF verifier st $TIME(R_n^{COMPR}) \leq p(\lambda + n)$

↳ some universal polynomial.

MIP^*
MIP^{com}
MIP^{ns} = EXPTIME

$(\lambda N)^\lambda$

(b) If V is a NF λ-bounded verifier,
then $\forall n \geq n_0$ and $N = f(n)$

time exp(n) $\qquad$ poly(n)

(i) If $\omega^*(V_N) = 1$ then $\omega^*\left((V^{COMPR})_n\right) = 1$

(ii) $\mathcal{E}\left((V^{COMPR})_n, \frac{1}{2}\right) \geq \max\left\{ \boxed{\mathcal{E}(V_N, \tfrac{1}{2})}, \boxed{N} \right\}$.

Rk: Running COMPR on a trivial $\overline{V}$ st V always accepts has a nontrivial outcome due to (i) and (ii)

(i) $\Rightarrow$ $\forall n$, $\omega^*\left((V^{COMPR})_n\right) = 1$

(ii) $\Rightarrow$ $\mathcal{E}\left((V^{COMPR})_n, \frac{1}{2}\right) \geq N$.

Completing the argument:

Fix TM M and $\lambda \geq 1$.

Define a NF verifier $V = V(M, \lambda)$ st on input 1^n

returns R_n st

$R_n(x, y, a, b)$ does the following:

$R_n(\underbrace{x, y, a, b}_{\{0,1\}^n})$ does the following:

1. Runs M for n steps. If M halts then R_n returns 1.

2. If M does not halt in $\leq n$ steps, then: Compute $\overline{V^{\text{COMPR}}} = \text{COMPR}(\overline{V}, \lambda)$

3. Return $(R^{\text{COMPR}})_n(x, y, a, b)$.

<u>Claim 1</u> $\forall$ TM M, $\exists$ integer $\lambda \geq 1$ (computable from M) st V defined above is λ-bounded.

<u>Proof</u> • estimate $|\overline{V}| = \text{poly}(\overline{M}) + \text{poly}(\lambda, \overline{\text{COMPR}}) + O(1)$

• estimate $\text{TIME}(R_n)$: $\text{poly}(|\overline{M}|, n)$ ← runtime of TM simulation

$+ \text{poly}(|\overline{V}|, \lambda)$ ← runtime of COMPRESS

$+ \text{poly}(\lambda + n)$ ← <u>by (a) in Claim</u>

$= \text{poly}(|\overline{M}|, n, \lambda) \leq (\lambda n)^\lambda$

$\forall n \geq 1$, and λ large enough wrt $|\overline{M}|$

Fix $\lambda = \lambda(|\overline{M}|)$ obtained from Claim 1.

<u>Claim 2</u> If M halt (on empty tape) then $\forall n \geq 1$, $\omega^*(G_n) = 1$

where $G_n(\pi_n = \mathcal{U}_n \times \mathcal{U}_n, R_n)$

$\mathcal{U}_n$: uniform over $\{0,1\}^n$

<u>Proof</u> Suppose that M halts in T steps.

If $n \geq T$ then R_n always accepts at step 1

$\Rightarrow \omega^*(G_n) = 1$.

If $n < T$ then R_n does not stop at step 1.

Then $w^*(R_n) = w^*((\cancel{R}^{\text{COMPR}})_n)$
by def of step 3.

Also, $\underline{w^*(V_{2^n}) = 1}$ if $2^n > T$.
by IH.

So by (a)(i) we also have $w^*(R_n) = 1$.

<u>Claim 3</u> If η does not halt then $w^*(G_n) \leq \frac{1}{2}$ $\forall n \geq 1$.

<u>Proof</u> Suppose not: $w^*(G_n) > \frac{1}{2}$ for some n. Then exists a strategy S for G_n st $w(G;S) \geq \frac{1}{2}$ and S uses finite dim ent, dim d.

However, by (b)(ii)

$$\mathcal{E}(G_n, \tfrac{1}{2}) \geq \max\{\underbrace{\mathcal{E}(G_N)}, N\}$$

$$> d \qquad \geq \max\{\mathcal{E}(G_{2^N}), 2^N\}$$

contradiction.

because R_{2^N} does not accept at step 1.

$$2^{2^{2^{\cdot^{\cdot^{\cdot^{2^N}}}}}} > d$$

Define $\tilde{F}$ as follows:

on input $\overline{\eta}$, $\tilde{F}$ computes λ according to Claim 1.

Then, $\tilde{F}$ returns game G_1 obtained from R_1

$V: 1, \overline{\eta}, \lambda$.

by Claim 2, η halts $\Rightarrow w^*(G_\eta) = 1$

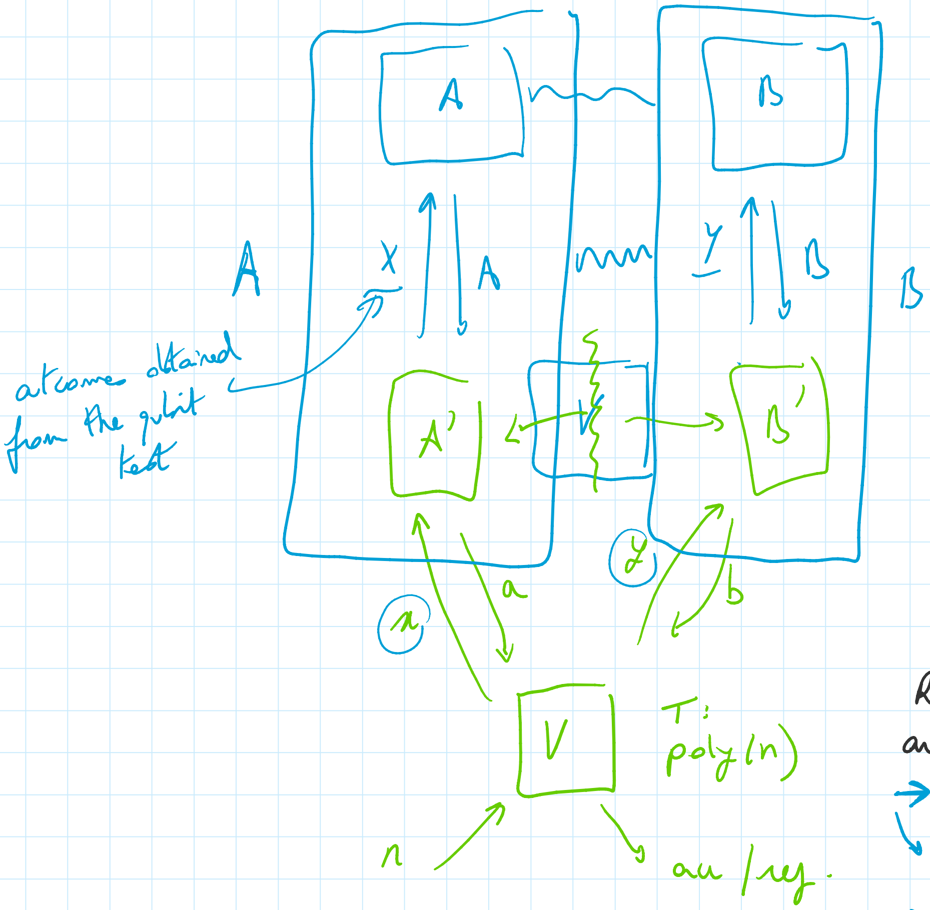
Claim 3, η does not halt $\rightarrow w^*(G_\eta) \leq \frac{1}{2}$

Designing the compression procedure:

Claim $\forall n \geq 1$, there is a game G_n that "test n qubits"

we'll use: if strategy S is st $\omega(G,S) \gg \frac{1}{2}$ (close to 1)

then S involves
- n-qubit Pauli observables
- n EPR pairs $|\phi^+\rangle^{\otimes n}$



V_N.

G_N: (i) select uniform random x, y

(ii) Get answers A, B

(iii) Verify using $R_N(x, y, A, B)$

Require that (x, y, a, b) are a proof that
(i) some x, y were generated uniformly
(ii) some A, B were obtained locally
(iii) $R_N(A, B, x, y) = 1$.