6.S979 Lecture 13

Interactive proof system:

NP decision problems

$\exists$ verification alg. V

YES instance $\Rightarrow \exists$ "witness" "proof" Π

completeness

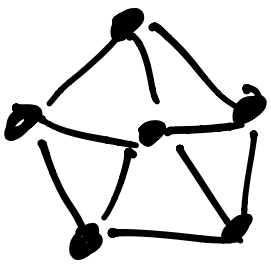
s.t. $V(\Pi) = 1$

NO instance $\Rightarrow \forall$ claimed proof Π

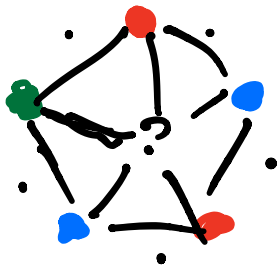
soundness

$V(\Pi) = 0$

E.g. graph 3-coloring

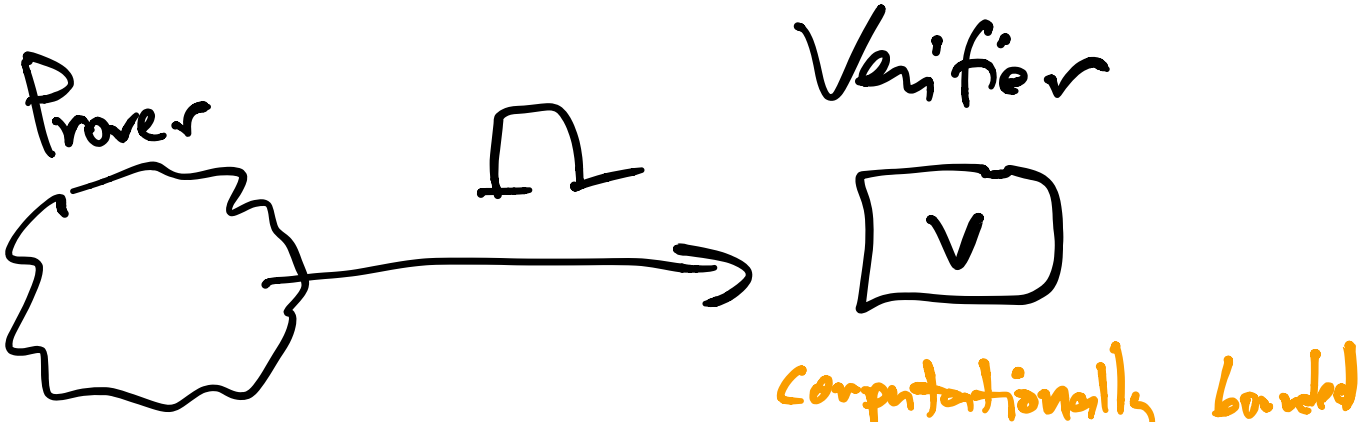


V will take in a coloring



$\leftarrow \Pi$

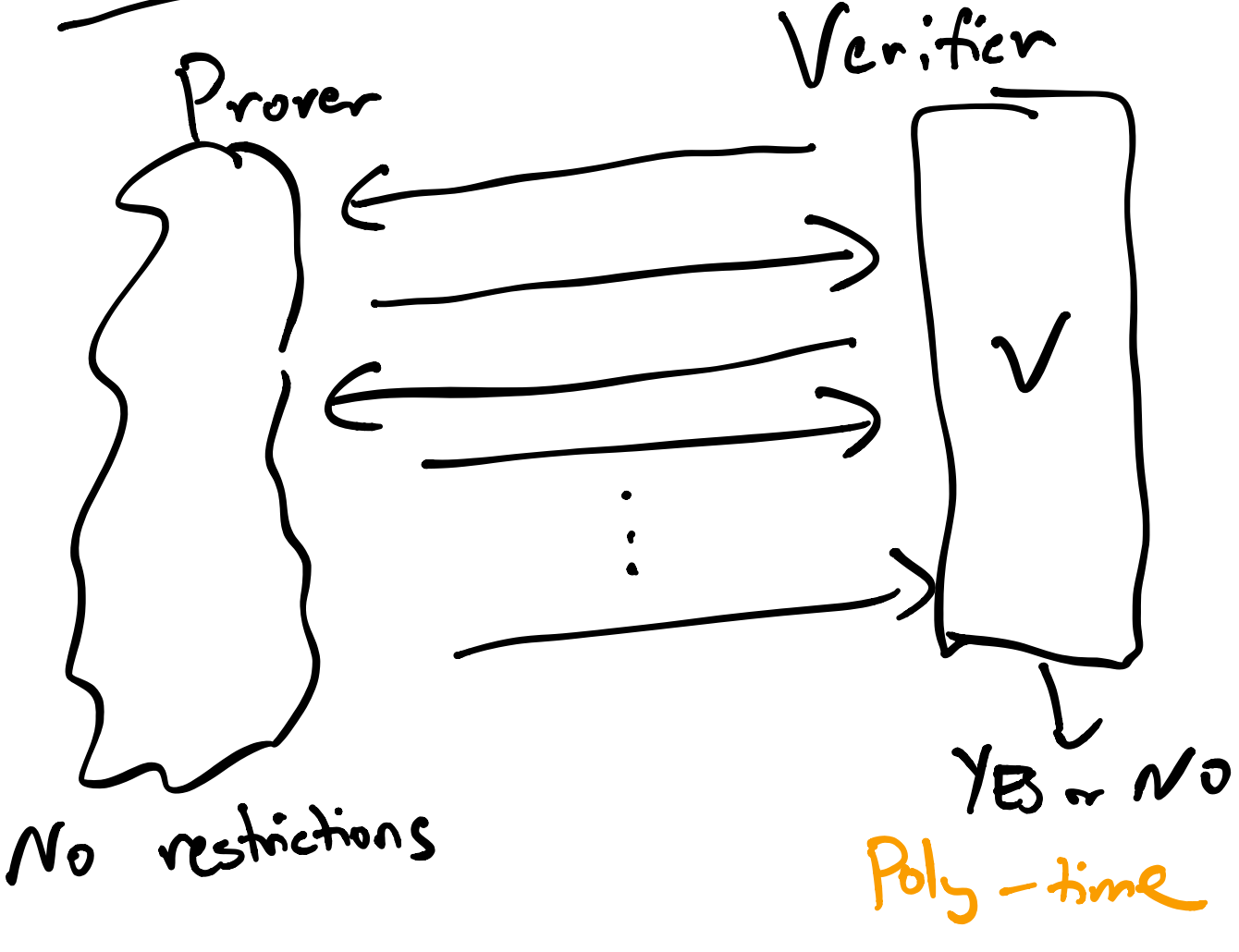
"proof system"



computationally bounded
(Poly-time)

No assumptions
(e.g. no computational assumptions)

IP (Interactive proofs)



No restrictions

Poly-time

Problem is in IP if ∃ verifier alg. V s.t.

Completeness: If YES,

∃ strategy for prover that makes V accept w/ prob $\geq 2/3$ ← any constant

$= c$

Soundness: If NO,

∀ strategies for prover.

$\text{Prob}[V \text{ accepts}] \leq 1/3$ ← s

(exercise: $s = 0$ reduces to NP) (I think!)

You can see that $NP \subseteq IP$

Thm: $IP = PSPACE$

↑

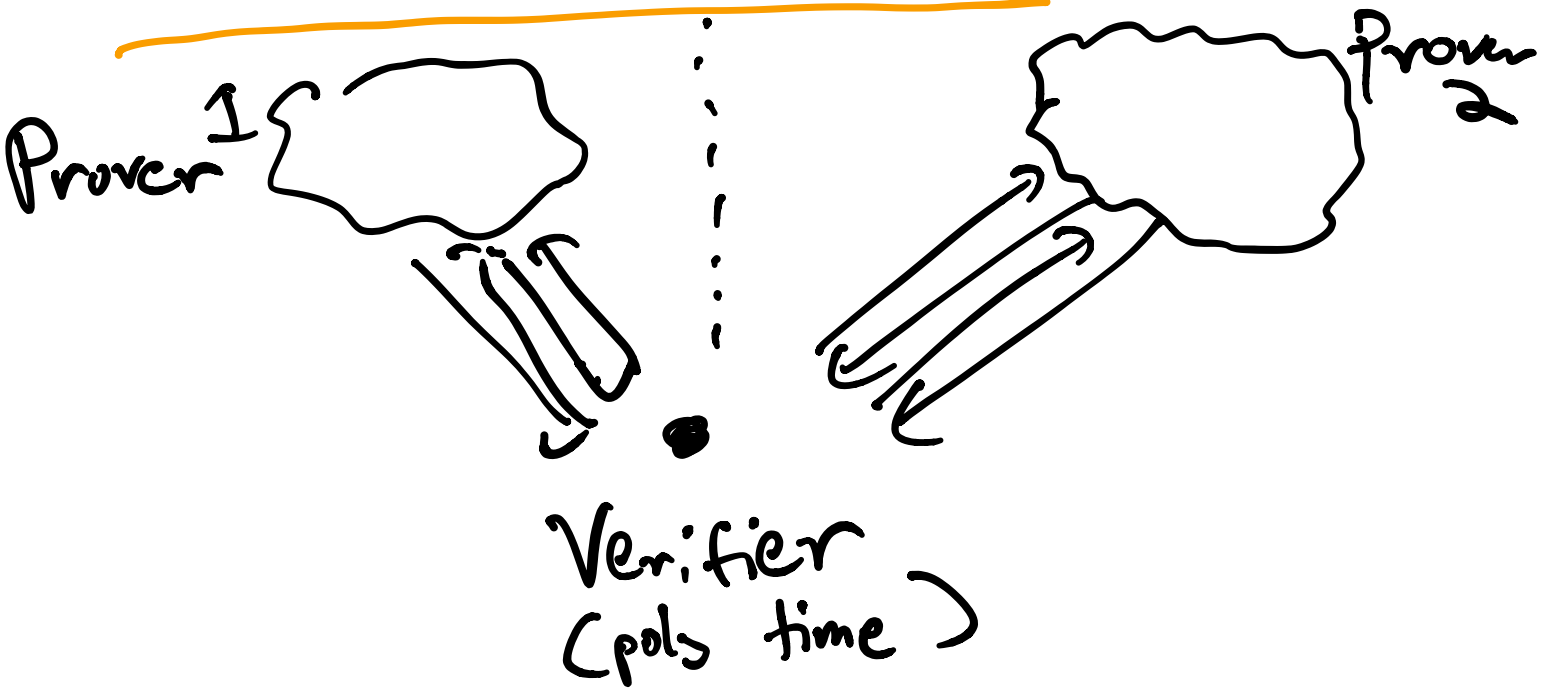
polynomial space

(Power of interaction / randomness)

IP = Oral Exam

NP = Written Exam

MIP (Multiprover interactive proof)



Completeness: YES case

$\exists$ strategy for provers

s.t. $\text{Prob}[V \text{ accepts}] \geq 2/3$

the provers can coordinate their strategies

Note: Provers are separated only during interaction w/ verifier

Soundness: NO

$\forall$ strategies for 2 provers

$\text{Prob}[V \text{ accepts}] \leq 1/3$

$IP \subseteq MIP$

(Because verifier can ignore prover #2)

Thm: $MIP = NEXP$

$NEXP$ = nondeterministic exponential time

NP w/ exp. time Verifier and exp size

$\cap$

(e.g. $\exists$ MIP protocol for 3-colorability of graphs of size 2^{n^2})

"Nonlocality" is a powerful computational resource

(separately interrogate criminals)

Succinct-3coloring:

Input: description of circuit C s.t. $C(\underbrace{i}_{n \text{ bits long}}, \underbrace{j}_{n \text{ bits long}}) = \begin{cases} 1 & \text{if } i \sim j \\ 0 & \text{if not} \end{cases}$

Fact: Succinct-3-coloring is NEXP complete

Pf: Use Cook-Levin

Aside: Discovered independently of Bell/CHSH/..., motivation was "zero-knowledge proofs"

MIP and non-local correlations

A strategy for provers in MIP is a point in $C_{\text{classical}}$

$$p(a,b \mid x,y)$$

provers' responses

verifier's questions

MIP protocol for language L

if $\forall x$,

Completeness: if $x \in L$ (YES input)

$\exists\ P_x \in C_{classical}$ ← $C_q / C_{qc} / C_{qa} / C_{qc}$

$\Pr_{P_x}[V_x \text{ accepts}] \geq 2/3$

Soundness:

if $x \notin L$ (NO input)

$\forall\ P_x \in C_{classical}$ ← $C_q / C_{qs} / C_{qa} / C_{qc}$

$\Pr_{P_x}[V_x \text{ accepts}] \leq 1/3$

Each correlation set gives us a variant of MIP

$MIP\{C_{classical}\} = MIP$

$MIP[C_{qa}] = MIP^*$

$MIP[C_{qc}] = MIP^{co}$

↑ commuting operator

Warning:

$C_1 \subseteq C_2$ does not imply $MIP[C_1] \subseteq MIP[C_2]$

Reason: Making C bigger gives provers more power

Completeness $\Downarrow$

Soundness $\Uparrow$

Example: [Cleve, Høyer, Toner, Watrous '04]

Suppose restrict verification algorithm $V(a, b \mid x, y)$

$= V(a \oplus b \mid x, y)$

(computational analog of XOR games)

$MIP^{\oplus}[C]$

$C_{classical} \subseteq C_{qa}$

Thm: 1) $MIP^{\oplus} = NEXP$

2) $MIP^{\oplus *} \subseteq EXP$ ← exponential time.

So if you believe $EXP \neq NEXP$ ($P \neq NP$) then $MIP^{\oplus *}$ is smaller than $MIP^{\oplus}$

Pf: 1) $MIP^{\oplus} = NEXP$ follows from PCP thm + Håstad

("crown jewel of complexity theory")

2) $MIP^{\oplus *} \subseteq EXP$

Use Tsirelson's characterization

Given input $\ell \in L$

$\exists$ V acting on XOR of provers' answers

If you can approximate

(*) $\max_{P \in C_q^{\oplus}} \text{prob}[V(P)]$

to error $\ll 1/3$, you can decide if $\ell \in L$.

Here's the Exp algorithm to solve (*)

1) $V \longrightarrow \vec{v}$ exp. long

$v_{x,y} = \text{prob}(x,y) \cdot S_{x,y}$

$V(a,b|x,y) = 1$ if $a \oplus b = S_{x,y}$

2) $\max_{p \in C_q^{\oplus}} \langle \vec{v}, p \rangle$

$= \max_{\Gamma} \operatorname{tr}\, \Gamma \cdot M_{\vec{v}}$

s.t.

$\Gamma \geq 0$

$\Gamma_{xx} = \Gamma_{yy} = I$

$\Gamma_{xy} = \Gamma_{yx}$

$\exp(n) \times \exp(n)$ sized matrix

This is a SDP & can solve in poly(dim) time $\ll$ EXP

Connection between correlation sets & MIP proof systems

1) Algorithm to maximize over C
$\Rightarrow$ upper bound on $MIP[C]$

2) Lower bound on $MIP[C]$
$\Rightarrow$ Hardness result for max over C

Obs: Suppose $C_{qa} = C_{qc}$

max over C_{qa} is **computable**

Alg: interleave
- inner approx. ($\to C_{qa}$) (brute force search) $\|$
- outer approx. ($\to C_{qc}$) (search over SoS certificates / NPA hierarchy)

$\Rightarrow$ $MIP[C_{qa} = C_{qc}]$ (contains only computable languages)

So if an undecidable language is in $MIP[C_{qa}] = MIP^*$

$\Rightarrow C_{qa} \neq C_{qc}$

Indeed, $MIP^* = RE$

$\Rightarrow C_{qa} \neq C_{qc}$