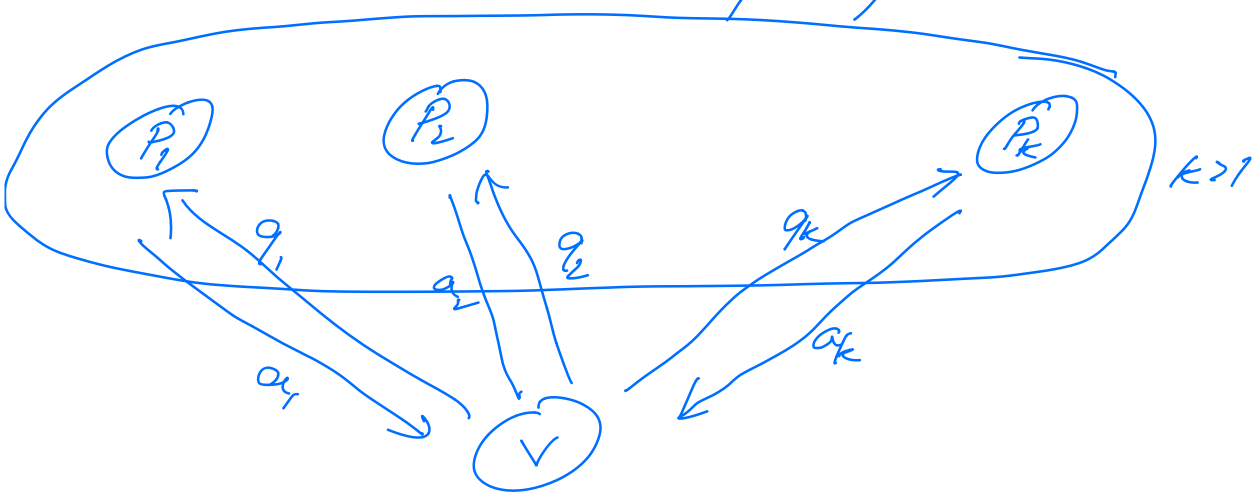
Today
- Multiprover Interactive Proofs (MIP)
- Intro to PCPs

CS5.203.1 Computational Complexity
- Lecture #28 (26 May 21)
Instructor: Prahladh Harsha

Multiprover Interactive Proofs.

[Ben Or-Goldwasser-Kilian-Wigderson]

What happens if the verifiers interacts with multiple provers?



Does having multiple prover help?

Possibly not, one can simulate multiple provers using a single prover.

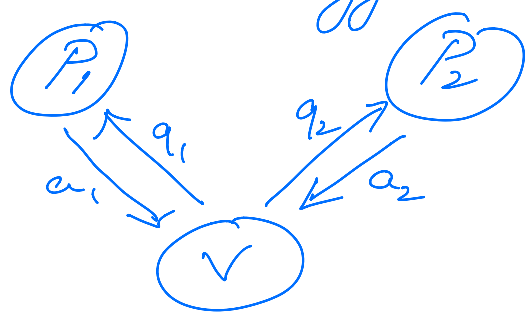
True, only if all provers are aware of each other's questions & answers.

MIP - multiprover proofs.

<u>Remarks:</u>

1. 2 provers suffice.

2. 1 round suffice



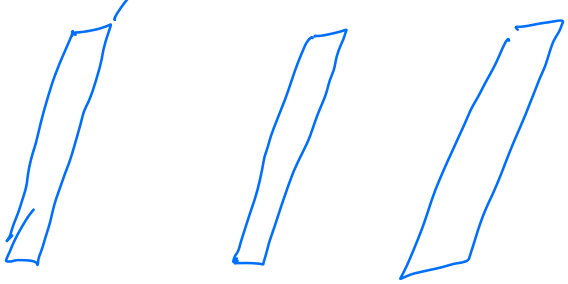
$V_1(x, R) \longrightarrow (q_1, q_2)$ | Private

$V_2(x, R, q_1, a_2) = acc/rej$ | Coins.

3. The answers can be just 1 bit each.

(perfect completeness - 3 provers needed).

One parallel round protocol



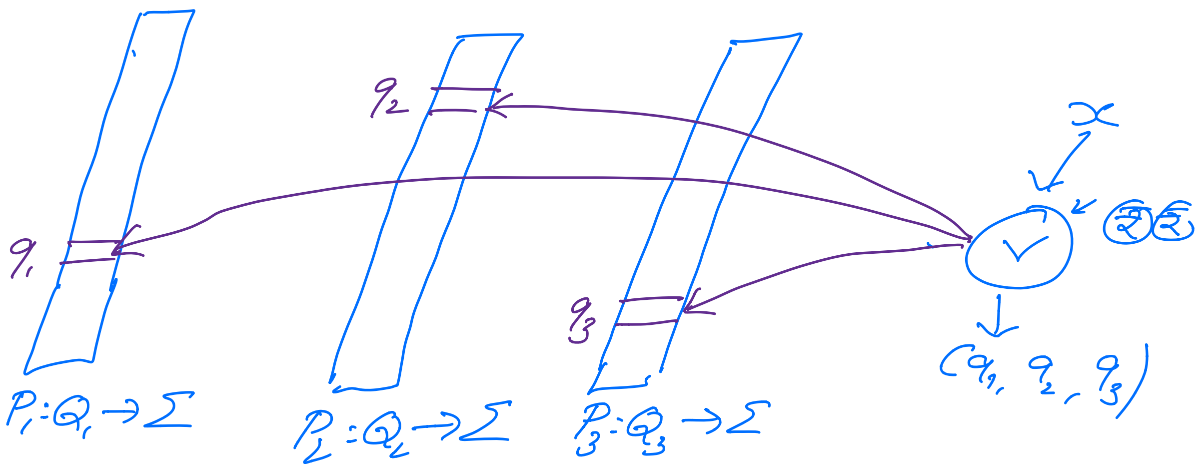
$P_i : Q_i \to \{0,1\}$

$Q_i(x)$ = set of questions to prover i.

Provers in 1-round protocols is just a fn

$P_i : Q_i \to \Sigma$ (Σ is the answer alphabet)

can be written down as a table of values in Σ.



P_i's are exponentially long.

<u>Thm</u> [BGKW, BF, RS, FS] $MIP \subseteq NEXP$

Thm [Babai-Fortnow-Lund]
$MIP = NEXP$

$\overline{MIP^*}$ = Provers are allowed to share entangled bits.

<u>Thm</u>: $MIP^* = RE$ [JNVWY]

Return to MIP = NEXP

Qn: Can the MIP result be scaled down logarithmically to yield a corresponding result for NP?

YES [...., BFLS, FGLSS, AS, ALMSS]

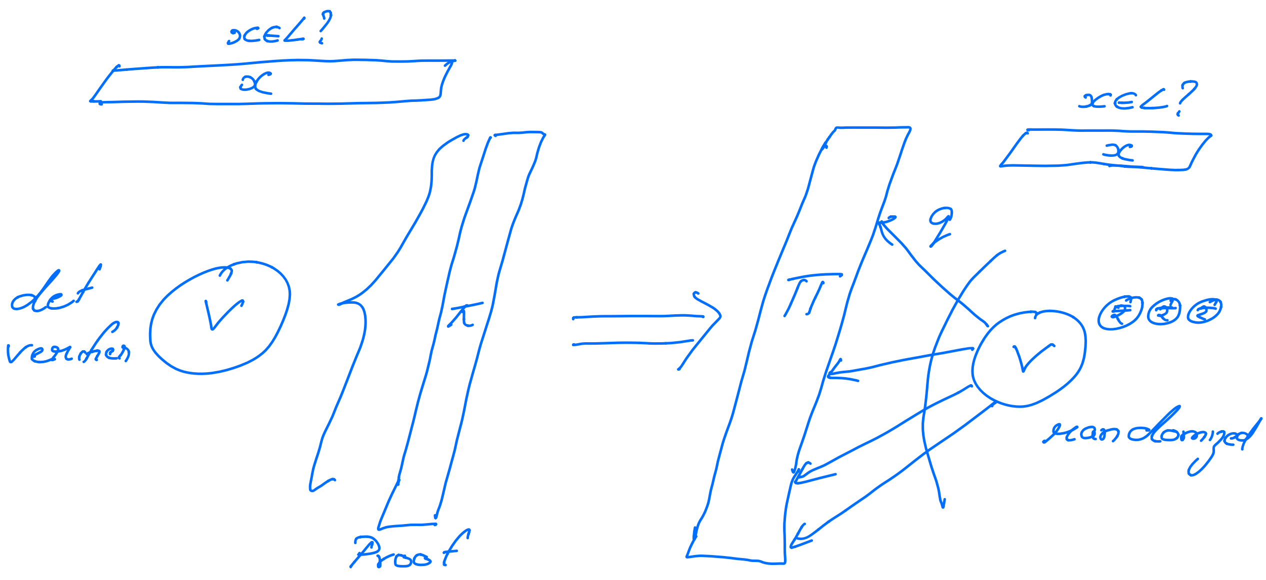
PCP Theorem

(Probabilistically Checkable Proofs)
(PCPs)

PCPs.

Recall classical definition of NP

$L \in NP$



$L \in NP$ if $\exists$ a ptime det verifier V s.t

$C: x \in L \Rightarrow \exists \pi,\ V(x,\pi) = 1$

$S: x \notin L \Rightarrow \forall \pi,\ V(x,\pi) = 0$

Key difference

(1) Strengthen verifier
det $\rightarrow$ randomized

(2) Weaken verifier
q-local view of proof

Formal Definition of Verifier.

Definition. (r,q,m,t,a)-restricted verifier (where $r,q,m,t,a: \mathbb{N} \rightarrow \mathbb{N}$)

is a prob TM that

on input x of length n

- tosses at most $r(n)$ random coins
- queries a proof of length $m(n)$ in at most $q(n)$ locations
- runs in time $t(n)$
- computes a predicate $D: \{0,1\}^{q(n)} \rightarrow \{acc, rej\}$ of size at most $a(n)$
- Accepts/rejects if the proof bits (restricted to $q(n)$ locations) satisfy the predicate.

$$V(x, R) \mapsto (\underbrace{Q}_{\text{set of queries}}, \underbrace{D}_{\text{predicate.}})$$

PCP class : $0 \le s < c \le 1$

$L \in PCP_{c,s}[r, q, m, t, a]$ if $\exists$ a (r, q, m, t, a) - rest verifier V s.t

Comp: $x \in L \Rightarrow \exists \pi \quad \Pr_R[D(\pi|_Q) = acc] \ge c$

Sound: $x \notin L \Rightarrow \forall \pi \quad \Pr_R[D(\pi|_Q) = acc] < s$

$$NP = \bigcup_c PCP[r = 0; q = n^c, m = n^c, t = n^c, a = n^c]$$

We will usually drop the parameter m, t, a

$m = 2^r \cdot q$
$t = \text{poly}$
$a = \text{poly}$

r - randomness
q - query complexity

$$NP = \bigcup_c PCP_{1,0}[r = 0, q = n^c]$$

$$BPP = \bigcup_c PCP_{\frac{2}{3}, \frac{1}{3}}[r = n^c ; q = 0]$$

MIP = NEXP can be stated as

$$NEXP = \bigcup_c PCP_{2/3, 1/3}[r = n^c, q = 2]$$

Scaling down.

PCP Theorem [BFLS, AS, ALMSS]
There exists a constant Q s.t. $\forall L \in NP$, there exists a constant c

$$L \in PCP_{1,1/2}[c\log n, Q].$$

Succinctly $NP = PCP[\log n, O(1)]$

<u>Remark</u>: ① $Q = 3$ $s: 1/2 \to 1/2 + \varepsilon$
$c: 1$

② $Q = 2$; $c = 1$; $PCP \subseteq P$

③ $PCP[o(\log n), O(1)] \subseteq P$

MAX3SAT.

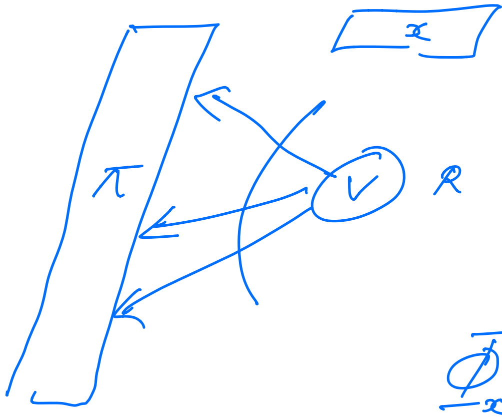
Input: $\varphi = C_1 \wedge C_2 \ldots \wedge C_m$

C_i = clause w/ 3 literals.

Goal: Find an assignment that satisfies the most number of clauses?

For starters, "assume" $Q = 3$

Predicate $= \underbrace{(\ \ \vee\ \ \vee\ \ )}_{\text{or}}$



$R \to i_1, i_2, i_3$

$C_R \triangleq (\pi_{i_1} \vee \bar{\pi}_{i_2} \vee \pi_{i_3})$

$$\underbrace{\Phi_x = \bigwedge_R C_R}_{\text{3CNF formula.}}$$

$x \longmapsto \Phi_x$

$x \in L \Rightarrow \Phi_x \in SAT$

$x \notin L \Rightarrow$ Every assignment violates at least ½ the clauses C_R