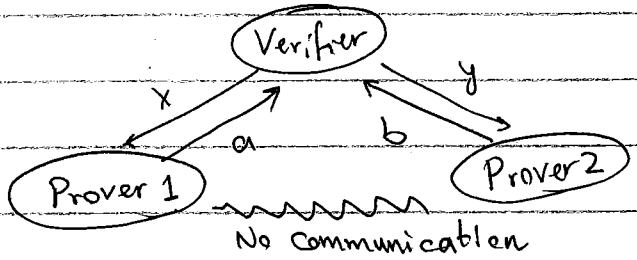
Parallel repetition:

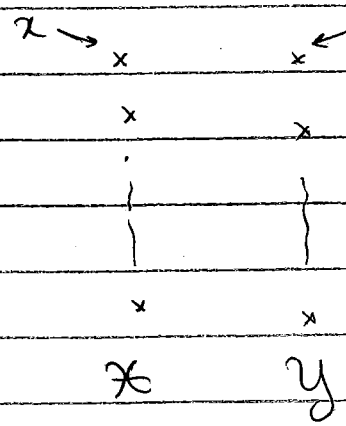
2-prover 1-round games (2P1R)



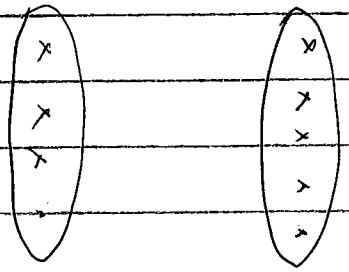
Verifier accepts if $V(x, y, a, b) = 1$.

Game: $V : X \times Y \times \Sigma \times \Sigma \longrightarrow \{0,1\}$, $|\Sigma| = q$.

Important in PCPs and inapproximability.



Example: ϕ : 3SAT instance.



X = clauses Y = variables of ϕ.

$V(C_j, x_i, \alpha, \beta) = 1$

if α satisfies C_j and

$$\alpha|_{x_i} = \beta$$

① If ϕ is satisfiable $\Rightarrow \exists$ strategy that makes $V=1$ w.p. 1.

② If every assignment fails to satisfy ρ fraction of the clauses, then no strategy can make $V=1$ w.p. $> 1 - \rho/3$.

Value of a game: $\omega(G) = \max_{\pi_1, \pi_2} \left[\Pr_{(x,y)\sim(X,Y)} \left[V(x, y, \pi_1(x), \pi_2(y)) = 1 \right] \right]$

($\omega(G)$: Val(G); G: the game; π_1, π_2: mapping from questions to answers.)

$$\begin{cases} \pi_1 : \mathcal{X} \to \Sigma \\ \pi_2 : \mathcal{Y} \to \Sigma \end{cases}$$

Comment: P_1, P_2 don't communicate, but can allow shared randomness.

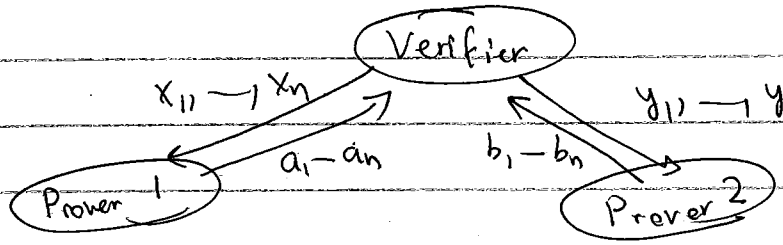
(shared randomness: R)

$$\text{thus, } \begin{cases} \pi_1 : \mathcal{X} \times R \to \Sigma \\ \pi_2 : \mathcal{Y} \times R \to \Sigma \end{cases}$$

* But shared randomness doesn't affect the value of the game.

* n- repeated games: Ask n independent questions in parallel:

Verifier samples $(x_1, y_1), \dots, (x_n, y_n) \sim (X, Y)$ iid.
(i.e., tensor product of the graph)



Accept iff $\bigwedge_{i=1}^{n} V(x_i, y_i, a_i, b_i) = 1$.

Question: $\omega(G^n)$ vs. $\omega(G)$?

Trivial: $\omega(G^n) \geq \omega(G)^n$

provers can answer just like G, independently.

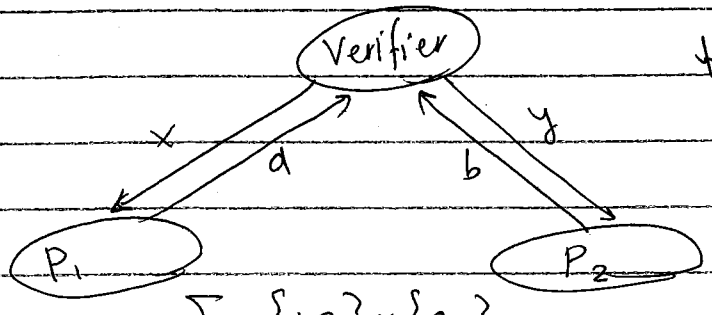
FRS '88 "claimed" that $\omega(G^n) = \omega(G)^n$
(i.e., parallel repetition = serial repetition.)

But the claim is false.

The answers can be correlated.

counter-**Example:** (Fortnow-Feige)

(X,Y) ~ u.a.r. bits

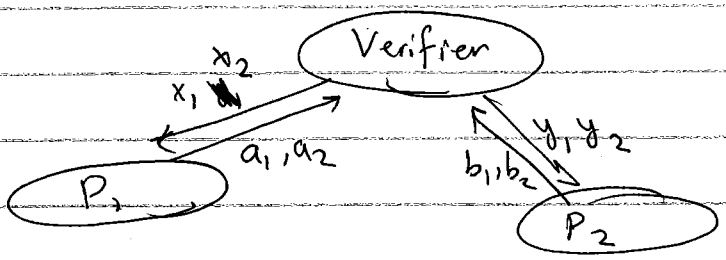


$V(x,y,a,b) = 1$ iff $a = b = (i,c)$
& P_i got bit c.

Note: $\omega(G) = 1/2$. (at least one prover must guess other prover's bit).

Now parallel repeat the game twice.

(X_1, Y_1), (X_2, Y_2) iid.



Can't do better than half (value can't increase in a repeated game).

But can do better than $1/4$.

W_i = win on question i:

$$Pr(W_1 \wedge W_2) = Pr(W_1)\, Pr(W_2 \mid W_1)$$

Strategy:

$a_1 = (1, x_1)$ $\quad b_1 = (1, y_2)$

$a_2 = (2, x_1)$ $\quad b_2 = (2, y_2)$

They win the first question if $x_1 = y_2$

Prob $= 1/2$.

But if so, we also win the 2nd round.

$\Rightarrow \omega(G^2) = 1/2$.

□

* By conditioning, the conditioned subsequent rounds can have "implicit communication"!

Exercise: If n=even, $\omega(G^n) = 2^{-n/2}$ for the above example.

* Parallel repetition theorem: (Raz'95)

$\forall$ games G, following holds:

If $\omega(G) = 1-\delta$, then

$$\omega(G^n) \leq 2^{-\Omega_{\delta,q}(n)}$$

known: δ^2 necessary!

In fact, $\omega(G^n) \leq 2^{-\Omega\left(\frac{\delta^3 n}{\log q}\right)}$

known: some dependence on q necessary!

$(q = |\Sigma|.)$

Comment: PCP theorem + Parallel repetition $\Rightarrow$ Strong inapproximability for the "label cover" problem, which implies many strong hardness results.

* Simplification of Raz'95 : Holenstein '07.

There's a new linear-algebraic proof too!

Lemma (Main):

$\exists\ \gamma = \gamma(q, \delta)$ s.t.

$\forall\ S \subseteq [n],\ |S| < \gamma n,$

$\Pr[W_S] \geq 2^{-\gamma n} \Rightarrow \exists\ i$ s.t. $\Pr(W_i \mid W_S) < 1 - \frac{\delta}{2}.$

Prob. of winning on all coordinates in S

This implies the theorem. Start with $S = \phi$ and increment it until the conclusion is violated or S becomes too large.

Pick $i_1, \ldots, i_\ell$ s.t. $\Pr(W_{i_j} \mid W_{i_1} \wedge \cdots \wedge W_{i_{j-1}}) \leq 1 - \frac{\delta}{2}$

$\Rightarrow w(G^n) \leq \max\left\{2^{-\gamma n}, \left(1 - \frac{\delta}{2}\right)^{\gamma n}\right\}.$

Proving the main lemma:

Intuition: Fix S. How to find i?

Use strategy for G^n to get one for G.
Suppose the conclusion is false.
Fix i. Given $(x, y) \sim (\mathcal{X}, \mathcal{Y})$,

Use shared randomness to generate $n-1$ other questions s.t. when (x, y) is placed in the i^{th} coordinate

and the rest of the questions in the other coordinates, s.t. the resulting distribution is statistically close to $(X_1, Y_1)(X_2 Y_2) \cdots (X_n y_n) \mid W_S$.

(because the assumption holds conditioned on winning on S).

Two main obstacles:

(1) Must have: $(X, Y) \underset{\text{close}}{\approx} (X_i, Y_i) \mid W_S$.

(even to make syntactic sense!)

$\Rightarrow$ Need such an i!

This is not so hard to overcome.

(using the fact that $\Pr(W_S)$ isn't too bad!)

(2) (Bigger Problem) How to fill in the values outside the i^{th} coordinate, without any communication?

(NB: (X, Y) might be correlated).

Idea: we can use "correlated sampling" as we saw (in a simple form) in the last lecture.