Today

- 2-prover PCPs / Label Cover
- Parallel Repetition Theorem

CSS. 330.1 : PCPs

Limits of Approximation Algorithms

Lecture 07 (2023-3-10)

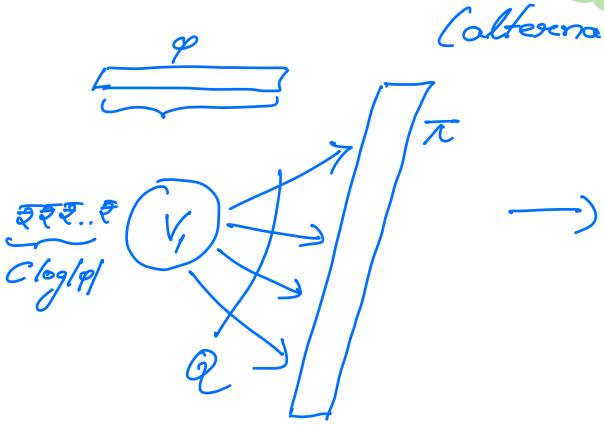
Instructor: Prahladh Harsha

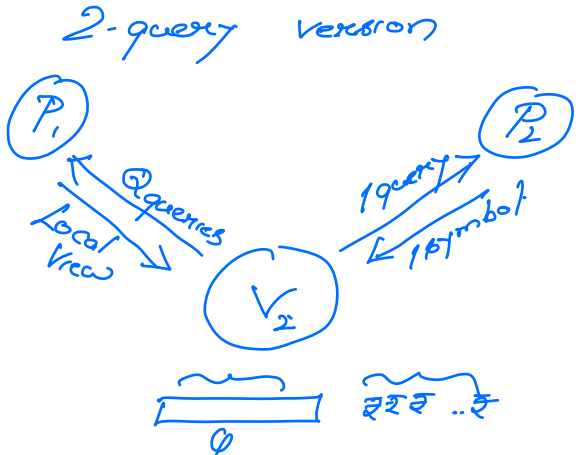
Recap from last time

PCP Theorem: There exist constants C, Q s.t.

$$SAT \in PCP_{1,\frac{1}{2}}[C\log n, Q]$$

(alternate characterization of NP)





V_2: Accepts if

(1) Local view from P_1 is an acc view for V_1.

(2) P_2's answer is consistent w/ P_1.

V_1's Completeness $\Rightarrow$ V_2's completeness.

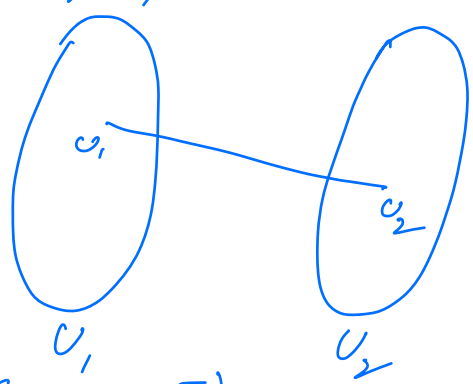
Soundness:

π - Ge the proof P_2 answers according to

$$\Pr_R[V_1^{\pi}(\varphi) = acc] \le \tfrac{1}{2} \Rightarrow \Pr_R[V_2^{P_1', P_2}(\varphi) = acc]$$
$$\le \frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{2Q}\right)$$
$$= 1 - \frac{1}{2Q}.$$

Robust-Soundness of V_1 $\Rightarrow$ Soundness of V_2 (w/o any deterioration w.r.t Q).

2-query PCP



$((V_1, V_2), E)$

$\Sigma_1 = \Sigma^Q$ $\quad$ $\Sigma_2 = \Sigma$

V_i = Set of possible queries to prover P_i.

$(v_1, v_2) \in E$ if $\exists$ a random coins R_1, V_2 queries (P_1, P_2) the queries (q_1, q_2)

For each $e = (v_1, v_2) \in E$ there is a predicate $\pi_e : \Sigma_1 \times \Sigma_2 \to \{0,1\}$.

Instance of Label cover.

$$\Phi = ((V_1, V_2), E, \Sigma_1, \Sigma_2, \Pi = \{\pi_e \mid e \in E\})$$

$$val(\Phi) = \max_{a_i : V_i \to \Sigma_i} \Pr_e[\pi_e(a_1(v_1), a_2(v_2)) = 1]$$

Alternate way of stating PCP Thm:

$gap_{c,s}$-LABELCOVER: { YES: Instances Φ s.t $val(\Phi) \geq c$
NO: Instances Φ s.t $val(\Phi) < s$

PCP Thm [in terms of Label Cover] $\exists \varepsilon \in (0,1)$
There is a polytime reduction from SAT to $gap_{1,\varepsilon}$-LC w/ constant sized alphabets Σ_1, Σ_2.

Focus of today's lecture:
Can we improve the soundness of the target LC instance in the above reduction?

Two possible routes
(1) Construct PCPs w/ very good, expected soundness
(2) Massage above reduction to improve soundness

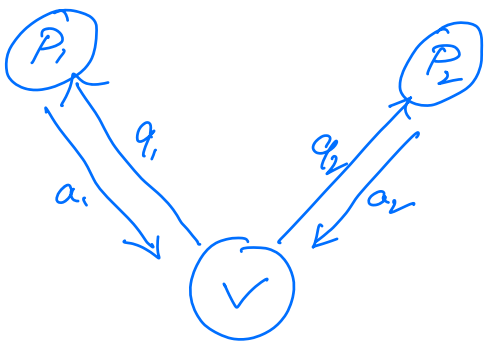
Today (2) via repetition.

k-Repetition does improve soundness
{ $s \to s^k$ ☺
2-query $\to$ 2^k-query ☹

Can we repeat maintaining 2-query structure.

Parallel Repetition.

G: $\mu \sim Q_1 \times Q_2$
(edge distribution)
π_e, $e \in E$



① $(q_1, q_2) \sim \mu$

② Accept if $\pi_{(q_1,q_2)}(a_1, a_2) = 1$

Value of Game:
Strategy for Provers

$\pi_1 : Q_1 \times R \to \Sigma_1$

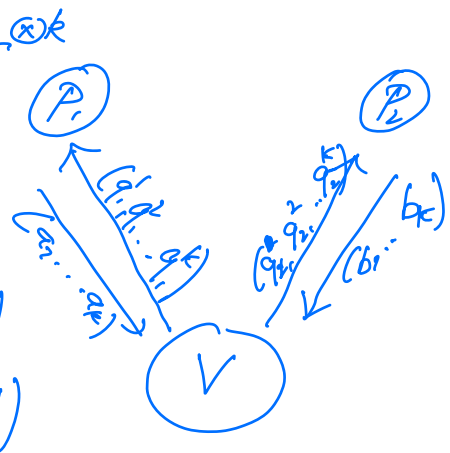
$\pi_2 : Q_2 \times R \to \Sigma_2$

$$\omega(G) = \max_{\pi_1, \pi_2} \Pr_{\substack{e=(q_1,q_2)\sim\mu \\ x \sim R}} \left[\pi_e(\pi_1(q_1, x), \pi_2(q_2, x)) = 1 \right]$$

k-parallel repeated Game. $G^{\otimes k}$

① For $j \in [k]$
$q_j = (q_1^{(j)}, q_2^{(j)}) \sim \mu$

② Queries P_1 w/ $(q_1^{(1)}, q_1^{(2)}, \ldots, q_1^{(k)})$
P_2 w/ $(q_2^{(1)} \ldots q_2^{(k)})$



(3) Receives answers $(a_1 \ldots a_k)$ from P_1
$(b_1 \ldots b_k)$ from P_2

(4) Accepts if $\forall j \in [k]$, $\pi_G(a_j, b_j) = 1$

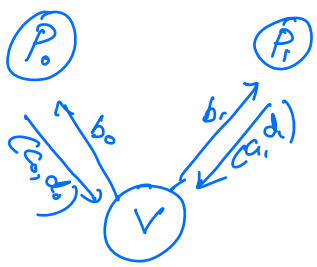
Qn: $\omega(G^{\otimes k})$ vs $\omega(G)$?

[Fortnow, Rompel, Sipser] (mistakenly) $\omega(G^{\otimes k}) = (\omega(G))^k$

Fortnow then came up w/ counterexample to above stmt.

Feige's Counterexample:

F:



(1) $(b_0, b_1) \leftarrow_R \{0,1\}^2$

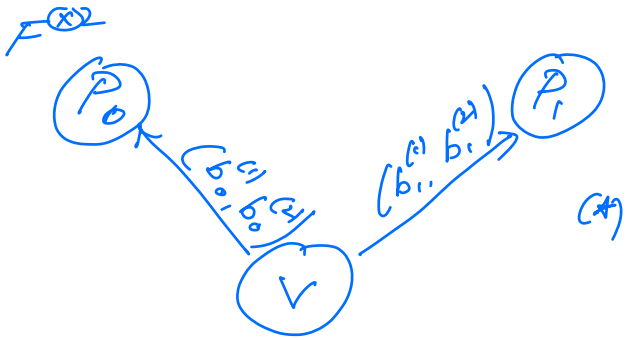
(2) Send b_i to prover P_i

(3) Receive answers (c_i, d_i) from Prover P_i

(4) Accept if
(i) $(c_0, d_0) = (c_1, d_1) (= (c, d)$ say$)$
(ii) Prover P_c send query d

Easy to see $\omega(F) = \frac{1}{2}$.

What about $\omega(F^{\otimes 2})$?



Consider the following strategy

(*) Prover P_1 on query $(b_0^{(1)}, b_0^{(2)})$ returns $((0, b_0^{(1)}), (1, b_0^{(2)}))$

(*) Prover P_2 on query $(b_1^{(1)}, b_1^{(2)})$ returns $((0, b_1^{(2)}), (1, b_1^{(2)}))$

For this strategy.

$$\Pr[V \text{ accepts}] = \Pr[b_0^{(1)} = b_1^{(2)}] = 1/2.$$

ie, $\omega(F^{\otimes 2}) \geq 1/2$.

Infact, $1/2 \leq \omega(F^{\otimes 2}) \leq \omega(F) = 1/2$.

Thm [Feige] $\omega(F^{\otimes k}) = \left(\frac{1}{2}\right)^{\lfloor \frac{k}{2} \rfloor}$

Qn: Does the $\omega(G^{\otimes k})$ decay w/ k?

[Feige-Kilian] For all G s.t $\omega(G) \leq 1-\varepsilon$.

Σ constant sized alphabets

$$\omega(G^{\otimes k}) \leq \frac{1}{\text{poly}(k)}.$$

[Raz '96] $\exists C$ $\forall \varepsilon \in (0,1)$ & $c \geq 1$, $\forall$ games G w/ ans size c/ε

$$\omega(G) \leq 1-\varepsilon \Rightarrow \omega(G^{\otimes k}) \leq \left(1 - \frac{\varepsilon}{100}\right)^{\varepsilon^{32} k / C}.$$

[Holenstein '07] $\omega(G^{\otimes k}) \leq \left(1 - \frac{\varepsilon}{2}\right)^{c\varepsilon^2 k/c}$.

Remarks: (1) Dependence on c is necessary (alphabet-size) [Feige-Verbitsky]

(2) Projection Games:

Predicate $\pi_e : \Sigma_1 \times \Sigma_2 \to \{0,1\}$

is actually of the form

$\pi_e : \Sigma_1 \to \Sigma_2$

Rao – projection games, - no dependence on alphabet size.

$\omega(G) \leq 1-\varepsilon \Rightarrow \omega(G^{\otimes k}) \leq \left(1 - \frac{\varepsilon}{2}\right)^{c\varepsilon k}$.

(3) Small-value games:

Dinur-Steurer - projection games

Braverman-Garg: general games.

(4) Proof Techniques:

FK: Combinatorial

Raz, Hol, Rao, BG: Information Theory

DS: Analytic / Linear-Algebraic.

(5) "Strong" Parallel Repetition

$\omega(G) \le 1-\varepsilon \Rightarrow \omega(G^{\otimes k}) \overset{??}{=} (1-\frac{\varepsilon}{2})^{\Omega(\varepsilon k)}$.

Raz '10 : Counterexample even for unique games.

Applications: Covering $\mathbb{R}^d$ w/ spheres.

Part II

Holenstein '07 : $\forall \delta$, alphabets Σ_1, Σ_2, there exists $\mu = \mu(\delta, |\Sigma_1|, |\Sigma_2|) \ge C\delta^2/\log(|\Sigma_1|\cdot|\Sigma_2|)$ s.t.

$\omega(G) \le 1-\delta$, then $\forall k$, $\exists \mu k$ coordinates $S \subseteq [k]$ s.t. $\Pr[\bigwedge_{i \in S} W_i] \le (1-\delta/2)^{\mu k - 1}$

where W_i = "i-repetition is satisfied."

Hence, $\omega(G^{\otimes k}) \le (1-\delta/2)^{\mu k}$

Lemma: $\forall S \subseteq [k]$, $\forall i \in [k] \setminus S$,

$\omega(G) + \varepsilon_i \triangleq \Pr[W_i \mid W_S]$ where $W_S = \bigwedge_{j \in S} W_j$

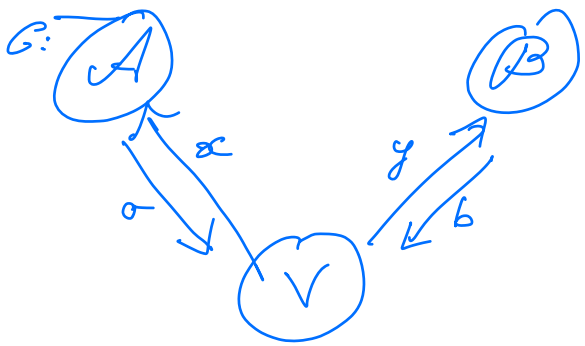
then $\mathop{\mathbb{E}}_{i \notin S}[\varepsilon_i] \le O\left(\sqrt{\frac{1}{k-|S|}\left(k\log(|\Sigma_1|\cdot|\Sigma_2|) + \log\left(\frac{1}{p_S}\right)\right)}\right)$

where $p_S = \Pr[W_S]$.

— $S = \{i_1, \ldots, i_m\}$

$$\Pr\left[\bigwedge_{i \in S} W_i\right] = \Pr[W_{i_1}] \cdot \Pr[W_{i_2} \mid W_{i_1}] \cdot \Pr[W_{i_3} \mid W_{i_1} \wedge W_{i_2}] \cdots \Pr\left[W_{i_m} \mid \bigwedge_{j<m} W_{i_j}\right]$$

— Theorem follows from Lemma.



Convenient to use this

Proof Strategy

"Embeds this query into the i-th co-ordinate of a k-repeated queries s.t provers can on co-ordinates S"

Fix the k-repeated prover strategies

$A: X^k \to \Sigma_1^k$

$B: Y^k \to \Sigma_2^k$

$X_1 \ldots X_k \xrightarrow{A} A_1 \ldots A_k$

$Y_1 \ldots Y_k \xrightarrow{B} B_1 \ldots B_k$

$(X_i, Y_i) \sim \mu$ ind across i

$\bar{A} = A(\bar{x})$

$\bar{B} = B(\bar{y})$

W_i: "$V(X_i, Y_i, A_i, B_i) = 1$"

W_S: $\bigwedge_{i \in S} W_i$

—

On input $(x, y) \sim (X, Y)$

P_A: Embed x into $\bar{x} = (x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots x_k)$

P_B: Embed y into $\bar{y} = (y_1 \ldots y_{i-1}, y, y_{i+1} \ldots y_k)$

using some common randomness r and then answer according to A & B

Suppose the common randomness R satisfies

$$\mathop{\mathbb{E}}_{(x,y)\leftarrow(X,Y)} \mathop{\mathbb{E}}_{r\in R}\left[\left(\bar{x}\big|_{x_i=x,\,R=r},\ \bar{y}\big|_{y_i=y,\,R=r}\right)\right] \equiv (\bar{X},\bar{Y})\big|_{W_S}$$

then $\Pr[W_i|W_S] \le \omega(G)$.

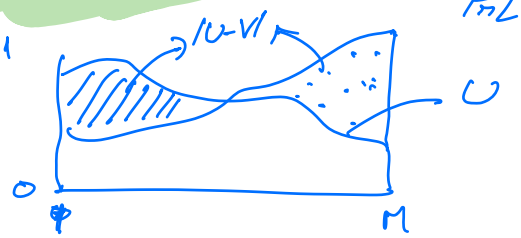
Basic Information Theory:

Relative Entropy ($\leftarrow$ KL-divergence)

U, V - distributions over M

$$D(U\|V) = \sum_{u\in M} \Pr[U=u]\cdot \log\frac{\Pr[U=u]}{\Pr[V=u]}$$

$$|U-V| = \max_{T\subseteq M} \Pr[U\in T] - \Pr[V\in T] = \frac{1}{2}\sum_{u\in M}\left|\Pr[U=u] - \Pr[V=u]\right|$$



Fact (1) $D(U\|V) \ge 0$

(2) Pinsker's Inequality:

$$D(U\|V) \ge |U-V|^2$$

Claim: V – r.v.; E – event; $\Pr[E] \geq 2^{-d}$

$\tilde{V} \triangleq V|_E$, then

$D(\tilde{V} \| V) \leq d.$

Pf: $D(\tilde{V}\|V) = \sum_v \Pr[V=v|E] \cdot \log \frac{\Pr[V=v|E]}{\Pr[V=v]}$

$= \sum_v \Pr[V=v|E] \log\left(\frac{1}{\Pr[E]} \cdot \frac{\Pr[V=v \wedge E]}{\Pr[V=v]}\right)$

$\leq d.$

Claim: $\bar{V} = V_1 \dots V_n$, $\bar{U} = \underbrace{U_1 \dots U_n}_{\text{product}}$

$D(\bar{V}\|\bar{U}) \geq \sum_{i=1}^{n} D(V_i \| U_i)$

Proposition: $\underbrace{U_1 \dots U_n}_{\text{product}}$, E – event $\Pr[E] \geq 2^{-d}$

then $\mathop{\mathbb{E}}_i\left[\left|U_i|_E - U_i\right|\right] \leq \sqrt{\frac{d}{n}}$

Proof: $\mathop{\mathbb{E}}_i\left[\left|U_i|_E - U_i\right|\right]^2 \leq \mathop{\mathbb{E}}_i\left[\left|U_i|_E - U_i\right|^2\right]$ (convexity of sq)

$\leq \mathop{\mathbb{E}}_i\left[D(U_i|_E \| U_i)\right]$ (Pinsker)

$= \frac{1}{n} \sum_i D(U_i|_E \| U_i)$

$$\leq \frac{1}{n} D(\bar{U}_E \| \bar{U}) \leq \frac{d}{n}$$ } Claims from above ☒

Want to construct a r.v $R = R(i)$ such that

(1) For each $r \in \text{Supp}(R)$.

$$(\bar{X}, \bar{Y}) \Big|_{X_i = x;\ Y_i = y;\ W_S \wedge R = r} = X\Big|_{X_i = x,\ W_S \wedge R = r} \times Y\Big|_{Y_i = y,\ W_S \wedge R = r}$$

(2) $R|_{X_i = x \wedge Y_i = y}$, $R|_{X_i = x}$, $R|_{Y_i = y}$ } are all close to each other.

Correlated Sampling: [Holenstein Sampling]

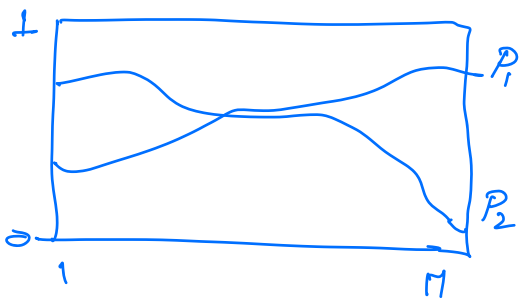
Thm: There exists a sampling procedure A such that for any ℓ dist $P_0 \ldots P_\ell$. $\forall$ dist B_i-sample obtained by running A on P_i such that the following holds

(i) $B_i \sim P_i$, $\forall i \in [\ell]$

(ii) $Pr[B_i \neq B_0] \leq 2\xi_i$ where $\xi_i = |P_0 - P_i|$

(iii) $Pr[\text{all } B_i\text{'s are identical}] \geq 1 - 2\sum_{i=1}^{\ell} \xi_i$

Pf:



Use common randomness as uniform samples from $M \times [0,1]$

A: On input $(i_1, \alpha_1), (i_2, \alpha_2) \ldots (i_t, \alpha_t), \ldots$

output j_ℓ s.t $\ell = \text{argmin}\{t \mid \alpha_t \leq p(i_t)\}$

⊠

Construction of Random Variable R.

R: (1) Answers for Alice & Bob's input on co-ordinates in S.
i.e, $(A_i, B_i \mid i \in S)$.

(2) Questions for coordinates in S
$(X_i, Y_i \mid i \in S)$

(3) A random A/B question
i.e,

$(V_i \mid i \notin S)$ $\quad V_i \sim_0 \{A, B\}$

$(T_i \mid i \notin S)$ $\quad T_i \leftarrow \begin{cases} X_i & \text{if } V_i = A \\ Y_i & \text{if } V_i = B \end{cases}$

$$R = (AB)\big|_S \, (XY)\big|_S \, (VT)\big|_{\bar{S}}$$

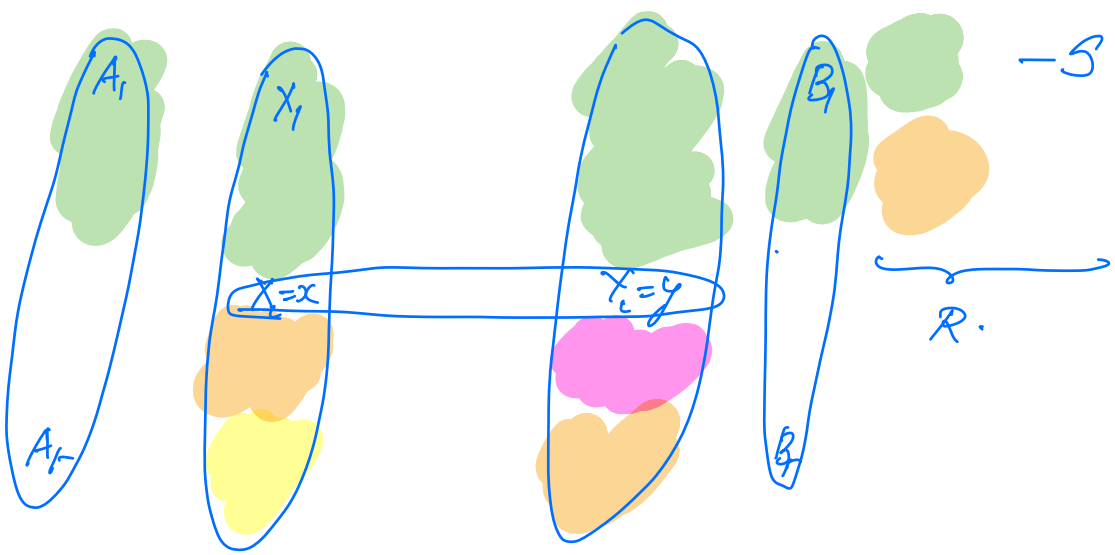
This R satisfies

For each $r \in \mathrm{Supp}(R)$.

$$(\bar{X}, \bar{Y})\Big|_{X_i = x_i;\ Y_i = y_i;\ W_S \wedge R = r}$$

$$\| \qquad \ddots$$

$$X\Big|_{X_i = x_i,\ W_S \wedge R = r} \times Y\Big|_{Y_i = y_i,\ W_S \wedge R = r}$$



Easy to see Alice can sample from the appropriate conditional

Similarly Bob.

Next lecture:

$$R/_{X_i = x \wedge Y_i = y \wedge W_S} \simeq_{\xi_i} R/_{X_i = x \wedge W_S}$$

$$\simeq_{\xi_i} R/_{Y_i = y \wedge W_S}$$