CS229r: ITCS

Lecture 19

4/9/2019

Today: Parallel Repetition Theorem

Review: Last time

- 2-Prover Game $G = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \mu, V)$

  μ = dist on $\mathcal{X} \times \mathcal{Y}$

  $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0,1\}$

- Strategy $= (f, g)$ $\quad f : \mathcal{X} \to \mathcal{A}$ $\quad g : \mathcal{Y} \to \mathcal{B}$
- $\mathrm{Val}_{f,g}(G) = \mathbb{E}_{(x,y)\sim\mu}\left[V(x, y, f(x), g(y))\right]$; $\quad w(G) = \max_{f,g} \{\mathrm{Val}_{f,g}(G)\}$

Parallel Repetition : $G^{\otimes k} = (\mathcal{X}^k, \mathcal{Y}^k, \mathcal{A}^k, \mathcal{B}^k, \mu^k, V^{\otimes k})$

$$V^{\otimes k} = \bigwedge_{i=1}^{k} V(x_i, y_i, \cancel{f(x_i)}\, a_i, b_i)$$

Theorem [Raz]: $\forall \mathcal{A}, \mathcal{B}$, $\forall \epsilon > 0$, $\exists \delta > 0$ s.t. $\forall G$ with $w(G) \le 1-\epsilon$

$$\forall k, \quad w(G^{\otimes k}) \le (1-\delta)^k.$$

Lemma [Raz]: $\forall f,g$ $\forall S \subseteq [k]$ s.t. $|S| \le \gamma k$ & $\Pr[W_S] \ge 2^{-\gamma k}$

$\exists i \notin S$ s.t. $\Pr[W_i \mid W_S] \le 1 - \epsilon/2$

[W_S = Winning on coordinates in S]. $\quad \gamma = \gamma(\epsilon, \mathcal{A}, \mathcal{B})$

Remember the counterexample

- $\mathcal{X} = \{1,2\}$, $\mathcal{Y} = \{3,4\}$, $\mathcal{A} = \mathcal{B} = \{1,2,3,4\}$

  $\mu = \mathrm{Unif}(\mathcal{X} \times \mathcal{Y})$; $V(x,y,a,b) = 1$ iff "$a = b \in \{x,y\}$".

- $w(G) = \frac{1}{2}$; $w(G^{\otimes 2}) = \frac{1}{2}$; $w(G^{\otimes k}) = \left(\frac{1}{2}\right)^{k/2}$!

- Lessons (for Lemma): . Can pair games into sets $\{1,2\}, \{3,4\}, \ldots \{k-1,k\}$ & arrange so that $W_1 \Rightarrow W_2$; $W_3 \Rightarrow W_4$ etc.

  . So if $S = \{1,3,5,7,9\}$

  $\Rightarrow$ $i \notin \{1,2,3,4,5,6,7,8,9,10\}$!

  But $i = 11$ works !!

- Proof has to figure all this out.

- How to get the "i" asserted by Lemma? Some Conditions

  - Need $(X_i, Y_i)|_{W_S} \approx (X_i, Y_i) \sim \mu$

    (Intuitively reason $\Pr[W_i | W_S] < 1 - \epsilon/2$

    is ① $(X_i, Y_i)|_{W_S} \sim (X_i, Y_i)$

    ② Conditioning on W_S doesn't give much information about strategy on i^{th} coordinate.

    [More precisely Alice + Bob should be able to sample "$X_S, Y_S \mid W_S, \ldots X_i, Y_i$"

- Some "perverse" strategies to worry about:
  - (f,g) wins ~~on~~ on coordinate 1 iff $X_1 = X_2 = 0$ & $Y_1 = Y_2 = 0$

$W_1 \Rightarrow X_2 = Y_2 = 0$. $\quad (X_2, Y_2 \mid W_1) \neq (X_2, Y_2) \sim \mu$

  - (f,g) win on coordinate 1 iff $X_1 = X_2$ (& " 2) $Y_1 = Y_2$
    - But winning uncorrelated with (X_1, Y_1)
    - $(X_2, Y_2)|_{W_1} \equiv_d (X_2, Y_2)$

      But $\Pr[W_2 \mid W_1] = 1$.

Fixing Problem of $\text{Dist.}(X_i, Y_i \mid W_S)$ far from $\text{Dist}(X_i, Y_i)$

1. Lemma: for every event E, $S \subseteq [k]$, $|S| \leq \gamma \cdot k$

$$\cancel{\exists i \notin S} \quad \Pr_{i \notin S}\left[\delta\left((X_i, Y_i)|_E, (X_i, Y_i)\right) > ? \right] < ?$$

Path Standard: Divergence, Pinsker etc.

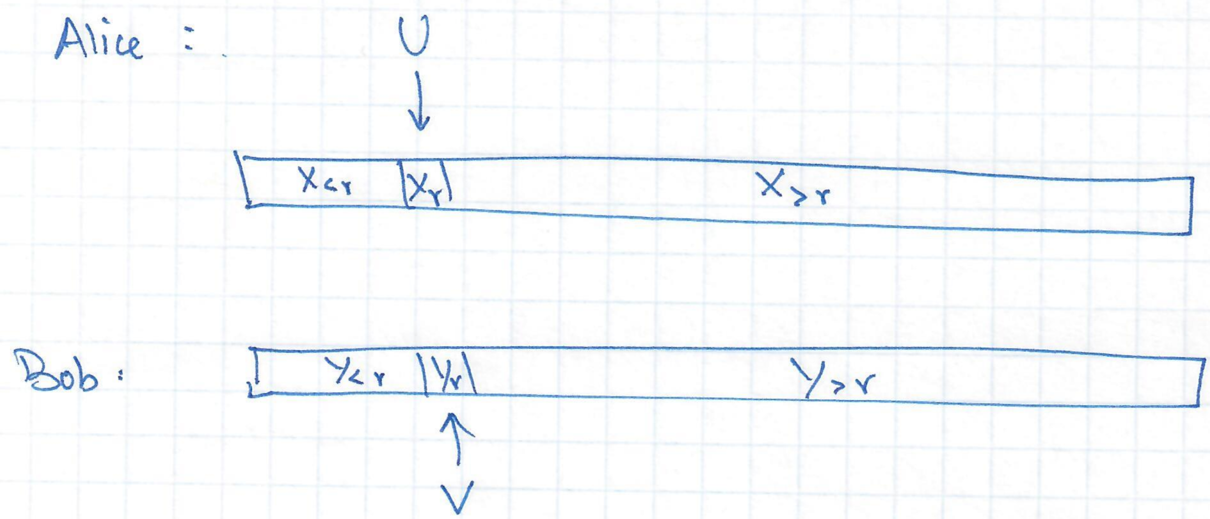
2. Task 2: $\exists i$ s.t. Alice + Bob can sample $X_S, Y_S \mid X_i, Y_i, W_S$ without communication.

Turning to Proof

Given : $(U,V) \sim \mu$ $\quad U \to$ Alice ; $V \to$ Bob

- Alice & Bob will try to use the protocol (f,g) for $G^{\otimes k}$ to solve (U,V). So they need to insert (U,V) into some coordinate.

- Assume w.l.o.g. that $S = \{1 \ldots r-1\}$
- Assume that we've permuted such that $(U,V) \to (X_r, Y_r)$



- How to generate (w.o. communication) $X_{<r}, X_{>r}$ & $Y_{<r}, Y_{>r}$?

- Very different issues.

(−) Need to pick $X_{<r}, Y_{<r}$ (and rest) so that first $<r$ coordinates accept! [Hard(er)]

(+) $X_{>r}, Y_{>r}$ just need to look good. No acceptance cond. [Easy(er)]

(+) r small compared to k [tiny constant fraction]

So can condition on $X_{<r}, Y_{<r}$ (or at least some aspects of these)

[Key Ingredient here: a Lemma]

(−) $k-r \approx k$ (so $X_{>r}, Y_{>r}$ v. large). Can't condition on these. So need some (correlated) sampling ideas.

Lots of technical challenges selecting i (eventually r) & S:

1. Need to condition on first $<r$ coordinates; let $E=$ denote this conditioning

2. Need $(X_r, Y_r)\big|_E \approx_\epsilon (U,V)$

3. Will use lots of correlating variables $T_r, T_{r+1} \ldots T_k = T_{>r}$ to coordinate choice of $X_{r+1} .. X_k$ & $Y_{r+1} \ldots Y_k$.
   - But ideal choice of $T_{r+1} .. T_k$ depends on (X_r, Y_r)
   - Alice only has X_r; Bob only has Y_r.

Need: $T_{>r} \mid X_r \approx_\epsilon T_{>r} \mid (X_r, Y_r) \approx_\epsilon T_{>r} \mid Y_r$.

Fortunately: IT to rescue; all above can be analyzed (easily)

once we have right [illegible]

Reduction:

1. Pick $x_1 \ldots x_{r-1}$ $\quad a_1 \ldots a_{r-1}$ "typically":
   $y_1 \ldots y_{r-1}$ $\quad b_1 \ldots b_{r-1}$

Typical: (i) if conditioned on $X_1 = x_1 \ldots Y_{r-1} = y_{r-1}$ & $f(X^k)_{<r} = a_{<r}$ ("C")
$g(Y^k)_{<r} = b_{<r}$

for 90% of $i > r$, $\Pr[W_i | C] \geq 1 - \frac{3\epsilon}{4}$.

(ii) Conditioned first $<r$ queries $= x_{<r}, y_{<r}$; answers are $a_{<r}, b_{<r}$ with prob $\geq \left(\frac{1}{|A|\cdot|B|}\right)^{-2k}$

2. Set $X_{<r} = x_{<r}$; $Y_{<r} = y_{<r}$; $X_r = U$; $Y_r = V$

3. Pick correlators distribution $\boxed{T_{>r} : T_j = (0/1, x_j/y_j)}$

- Let $\tilde{T}_{>r} \triangleq T_{>r} | W$ $\qquad W \triangleq (f(X^k)_{<r} = a_{<r})$
$\& (g(Y^k)_{<r} = b_{<r})$
$\triangleq W_1 \wedge \ldots \wedge W_k$

- Alice : sample $\tilde{T}_{>r} | X_r$
  Bob : sample $\tilde{T}_{>r} | Y_r$
  $\Big\}$ correlatedly.

4. Alice + Bob ~~complete~~ compute $X_{>r}$: $X_j = x_j$ if $T_j = 0$
$X_j \sim X_j |_{y_j}$ if $T_j = 1$

   Similarly Bob

5. Output: $f(X^k)_r$, $g(Y^k)_r$