CS229r: IT & CS
LECTURE 19

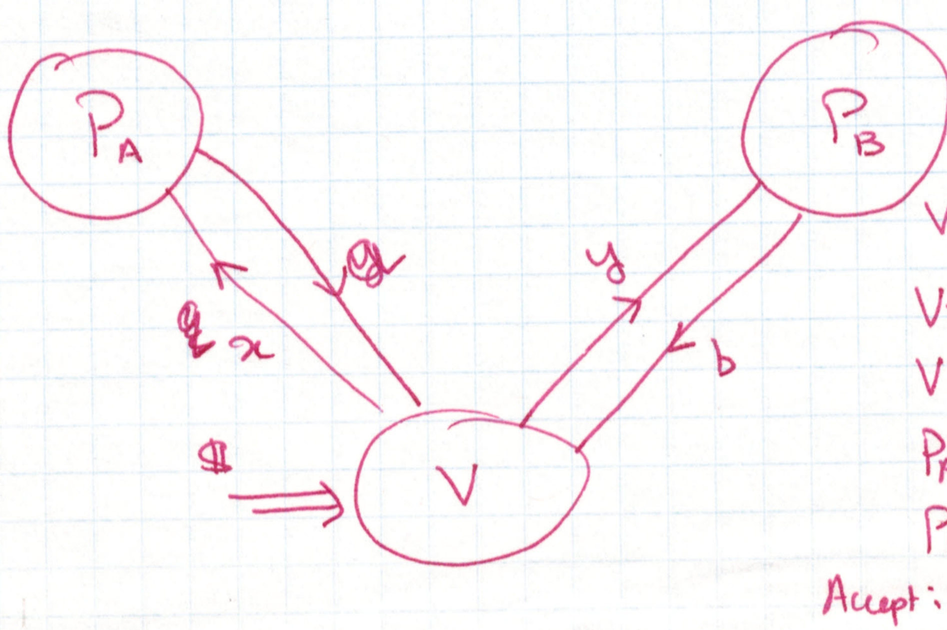
4/4/19

TODAY

- 2-PROVER PROOF SYSTEMS
- PARALLEL REPETITION
- MOTIVATION: Hardness of Approximation
- CONJECTURE + COUNTEREXAMPLE
- THEOREM (RAZ; HOLENSTEIN)
- TOWARDS PROOF

2-Prover Proof Systems Framework

2 provers + 1 verifier ⇒ 3 players in all



V: $(x,y) \sim \mu$.

$V \to P_A$: x

$V \to P_B$: y

$P_A \to V$: a

$P_B \to V$: b

Accept if $V(x,y,a,b) = 1$

In English

- 2 Provers ("Criminals") being interrogated by ("Interrogator") verifier; Verifier randomized.
- Provers strategize together, but can't exchange question being asked. Must answer questions without coordination
- Verifier determines their innocence/guilt based on answers.
- Q: What is max (over strategies) of ~~Prover's~~ Verifier's acceptance prob.

Formally: • Game = (μ, V) $\left\{ \begin{array}{l} \mu \text{ supported on } \mathcal{X} \times \mathcal{Y} \\ V: \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0,1\} \end{array} \right.$

- Strategy = $f: \mathcal{X} \to \mathcal{A}$, $g: \mathcal{Y} \to \mathcal{B}$

- value $(f,g) = \mathop{\mathbb{E}}_{(x,y) \sim \mu} \left[V(x, y, f(x), g(y)) \right]$

- Value(Game) $= \max_{f,g} \{ \text{value}(f,g) \}$.

Example: Odd-Cycle Game

- $G = (V, E)$ $\quad V = \mathbb{Z}_n$, $E = (i, i+1 \pmod n)$
- $\mu = \frac{1}{2}(\text{unif}(E) + \text{unif}(i,i))$
- $\mathcal{A} = \mathcal{B} = \{0,1\}$
- $V(x,y,a,b) = 1 \iff$ "$a=b \iff x=y$"

Claim: $\text{Value}(\text{Game}) = 1 - \Theta(\frac{1}{n})$. [Exercise?].

In English

- Provers claiming G is 2-colorable (odd cycle is not!)
- Verifier picks edge (u,v) & asks A for $X(u)$ & B for $X(v)$; accept if $X(u) \neq X(v)$.
- Unfortunately fails if Alice always says 0 & Bob " 1.
- So w.p. $\frac{1}{2}$ verify consistency $(X_{Alice}(u) = X_{BOB}(u))$ & w.p. $\frac{1}{2}$ verify edge
- Strategy: ~~Pick one edge to~~ $X(v) = v \pmod 2$.

Parallel Repetition Problem :

- Can Interrogator reduce prob. error by asking many questions?
  - Answer: yes : k-repetition $\Rightarrow$ value$(G)^k$.
- But : ~~can you~~ what if ~~they~~ interogator can only ask ~~an~~ a many-part question.

  [Interview vs. Written Exam]

- How does error. prob. behave?

Approximation Motivation

2-Prover Game $\equiv$ Generalized Graph k-Colorability

$(G=(V,E)$ & function

$V: E \times [k] \times [k] \to \{0,1\})$

(u,v) validly colored if

$V((u,v), X(u), X(v)) = 1$.

'92: Well-known : ~~$\exists$ Game~~ approximation Gen 3-Col is hard to with $1+10^{-10}$.

Can we get $\exists$ k s.t.

approximate Gen k-col. ~~to~~ withing 10^{10} is hard?

Parallel Repetition : ("Tensor Product", Repeated Game ...)
Amortization

$$G^{\otimes k} = (\mu^{\otimes k}, V^{\otimes k})$$

$\mu^{\otimes k} = \underbrace{\mu \times \mu \times \mu}_{k \text{ times}}$ supp on $\mathcal{X}^k \times \mathcal{Y}^k$.

$$V^{\otimes k}((x_1 .. x_k), (y_1 .. y_k), (a_1 .. a_k), (b_1 ... b_k)) = \bigwedge_{i=1}^{k} V(x_i, y_i, a_i, b_i)$$

"Repeating Questions in Parallel"

"Allows provers to "coordinate" answers"

is $\text{Value}(G^{\otimes k}) = \text{Value}(G)^k$?

Feige's Example

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

$\mu = \text{unif}(\mathcal{X} \times \mathcal{Y})$.

$V(x,y,a,b) = 1$ if $a = b$ & $a \in \{x,y\}$.

In English : Verifier ~~Picks~~ tosses two coins $x \in \{1,2\}$
$y \in \{3,4\}$

~~Pr~~

& sends to Alice & Bob. They must guess one of the coins. $\text{Value}(G) = 1/2$.

2-fold repetition

- Alice $\leftarrow \{x_1, x_2\}$ $\qquad$ $\{y_1, y_2\} \rightarrow$ Bob

  $\longrightarrow \{a_1, a_2\}$ $\qquad$ $\{b_1, b_2\} \longleftarrow$

- Accept if $\quad a_i = b_i$ & $a_i \in \{x_i, y_i\}$ for $i = 1, 2$.

- Strategy : " ~~Guess~~ Hope that $x_1 = y_2 - 2$ $\cancel{(\bmod 2)}$ "

$$\begin{cases} a_1 = x_1 \\ a_2 = x_1 + 2 \end{cases} \qquad \begin{aligned} b_1 &= y_2 - 2 \\ b_2 &= y_2 \end{aligned}$$

if Hope then win
else Lose

$\Pr[\text{Hope}] = 1/2$

$$\text{value}\left(G^{\otimes 2}\right) = \frac{1}{2} = \text{value}(G) \quad !!$$

Clearly Does not behave as expected.

Thm [Verbitsky]: $\forall G$ s.t. $\text{value}(G) < 1$, $\forall \epsilon > 0$ $\exists k$ s.t.

$$\text{value}\left(G^{\otimes k}\right) \leq \epsilon. \qquad [\text{very weak}]$$

Thm [Raz]: $\forall A, B, \epsilon > 0$ $\exists \epsilon' > 0$ s.t. $\forall G$ with $\text{value}(G) \leq 1 - \epsilon$

$$\forall k, \quad \text{value}\left(G^{\otimes k}\right) \leq (1 - \epsilon')^k.$$

[does not depend on $|X|$]

Would like to say: Fix $f, g : \mathcal{X}^k \times \mathcal{Y}^k \to A^k \times B^k$

$\forall i \ldots \Pr\left[V(x_i, y_i), f(x)_i, g(y)_i) = 1 \;\middle|\; V(x_j, y_j, f(x)_j, g(y)_j) = 1 \;\; \forall j \right] \leq 1-\epsilon$

Problem: x_i, y_i ind. of $(x_{<i}, y_{<i})$ but

$f(x)_i$, $f(y)_i$ is not ind. of

$(x_{<i}, y_{<i}\; f(x)_{<i}, g(y)_{<i})$

<u>More Intricate Lemma:</u>

$S \subseteq [k]$

<u>Notation</u>: W_S = Winning on S

= Event that f, g win on S.

$$\boxed{V(x_i, y_i), f(x)_i, g(y)_i) = 1 \quad \forall i \in S}$$

<u>Lemma:</u>

$\forall A, \epsilon\ \exists \gamma > 0$ s.t. $\forall G$ with value$(G) \leq 1-\epsilon$

$\forall S$ s.t. $|S| \leq \gamma k$

either $\Pr[W_S] \leq 2^{-\gamma k}$

or $\exists i \notin S \quad \Pr[W_i \mid W_S] \leq 1 - \epsilon/2$

Proof: Embedding. Next Lecture.