ITCS: CS229r 3/5/2019

LECTURE 11

COMMUNICATION COMPLEXITY LOWER BOUNDS

① INNER PRODUCT FUNCTION
② DISTRIBUTIONAL COMPLEXITY
③ DISCREPANCY
④ LOWER BOUND FOR IP
⑤ BEYOND PRODUCT DISTRIBUTIONS: SET DISJOINTNESS
⑥ INFORMATION COMPLEXITY

Last time.

Defined Comm. Comp. ~~Bound~~ Model: Alice ⇄ Bob, Alice has x, Bob has y

- $CC(f)$ = det. complexity of computing f = # bits exchanged
- Π = Protocol $\Pi(x,y)$: Output of protocol under input x, y.
- $CC^{Priv}(f)$; $CC^{Pub}(f)$ = complexity with private & public randomness.

$CC(f) \geq \log \text{rank}(M_f)$. How about $CC^{Pub}(f)$?

- **Inner Product function**

$$IP(x,y) \triangleq \sum x_i y_i \pmod 2$$

- $CC^{Pub}(IP) = \Omega(n)$. How do we prove this.
  - Rank insufficient! (bound (Identity) $= 2^n$; $CC^{Pub}(EQ) = O(1)$)
  - Idea 1 . . Put distribution μ on (X,Y)

$$D_{\epsilon,\mu}(f) \triangleq \min_{g \text{ s.t } \delta_\mu(f,g) \le \epsilon} \{CC(g)\}$$

$$\cdot \delta_\mu(f,g) \triangleq \Pr_{(x,y)\sim\mu}[f(x,y) \neq g(x,y)]$$

Claim: $CC^{Pub}(f) \geq \dfrac{D_{\epsilon,\mu}(f)}{\log 1/\epsilon}$

Proof: Don't need randomness if (x,y) random.

- Idea 2: ~~CC~~ "CC" $\leq$ "Discrepancy" $\leq$ "eigenvalue".

$M_{\mu,f}$: w.l.o.g. f: Domain $\to \{+1,-1\}$

μ also a matrix

$$M_{\mu,f}(x,y) = \mu(x,y) \cdot f(x,y).$$

- $\mathrm{Disc}(M) \triangleq \max_{\substack{S \subseteq \{0,1\}^n \\ T \subseteq \{0,1\}^n}} \left| \sum_{x,y} \mathbb{1}_S(x) \cdot \mathbb{1}_T(y) \cdot M(x,y) \right|$

  - if Π is a k-bit protocol for f with 0-error then $\mathrm{Disc}(M) \geq 2^{-k}$.

  - if Π is k-bit protocol for f with ϵ-error then $\mathrm{Disc}(M) \geq 2^{-k}(1-2\epsilon)$.

- $CC_{\mu,\epsilon}(f) \leq k \Rightarrow \mathrm{Disc}(M) \geq 2^{-k}(1-2\epsilon)$

  or $\mathrm{Disc}(M) < 2^{-k}(1-2\epsilon) \Rightarrow CC_{\mu,\epsilon}(f) > k$.

- <u>Idea 3</u>: $\mathrm{Disc}(M)$ vs. eigenvalues

$$\mathrm{Disc}(M) \leq \max_{\chi_S, \chi_T \in \{0,1\}^{2^n}} \sum_{x,y} \chi_S(x) \cdot \chi_T(y) \cdot M(x,y)$$

$$\leq \max_{\substack{u,v \in \{0,1\}^{2^n} \\ \|u\|_2, \|v\|_2 \leq 2^{n/2}}} u^T M \cdot v$$

$$= \lambda_{\max}(M) \cdot 2^n$$

$$\Rightarrow \lambda_{\max}(M) \leq 2^{-n-k} \Rightarrow \mathrm{Disc}(M) \leq 2^{-k} \Rightarrow CC_{\mu,\epsilon}(f) > k-1$$

μ = ? for IP ?

- Simply uniform. $\mu(x,y) = \frac{1}{4^n} \quad \forall x,y$
- ~~Disc~~ $\lambda_{max}(M_{\mu, IP(n)}) = ?$

$$M_{\mu, IP(n)} = M_{\mu_1, IP(1)}^{\otimes n}$$

$IP(1)(x,y) = x \cdot y \qquad x,y \in \{0,1\}$

$$M_{\mu_1, IP(1)} = \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & -1/4 \end{bmatrix}$$

$$\lambda_{max}\left(M_{\mu_1, IP(1)}\right) = \frac{1}{\sqrt{8}}$$

$$\lambda(M_{\mu, IP(n)}) = \lambda(M_{\mu_1, IP(1)})^n = \frac{1}{8^{n/2}} = \frac{1}{2^n} \cdot \frac{1}{2^{n/2}}$$

$\Rightarrow Disc(M) \leq 2^{-n/2} \Rightarrow \mathbb{E}D_{\mu, \frac{1}{4}}(IP) \geq \frac{n}{2} - 1$. ⊠

Is $n/2$ right? On uniform dist.?

How about worst-case?

Exercises...

Set Disjointness

$DISJ^n$: $DISJ^n(X,Y) = 1$ if $\exists\, i$ s.t. $X_i = Y_i = 1$

$= 0$ o.w.

$\left(DISJ^n(X,Y) = \bigvee_{i=1}^{n} (X_i \wedge Y_i) \right)$

Challenge with Disjointness: Want Distribution with $X \perp Y$

But then $|X|, |Y| \approx \sqrt{n}$ & in this case $\exists$ $\tilde{O}(\sqrt{n})$ bit protocol.

Exercise: Give an $\tilde{O}(\sqrt{n})$ protocol for all $\mu = \mu_X \times \mu_Y$.

History

- Babai-Frankl-Simon: $\Omega(\sqrt{n})$ on Unif distribution
- Kalyanasundaram + Schnitger: $\Omega(n)$ & on ?
- Razborov: $\Omega(n)$ on complex dist.
- Bar-Yossef-Jayram-Kumar-Sivakumar: $\Omega(n)$ on

$\mu_{XY} = (\mu_{X_i Y_i})^n$

$(X_i, Y_i) \perp (X_{-i}, Y_{-i})$!

Information Complexity

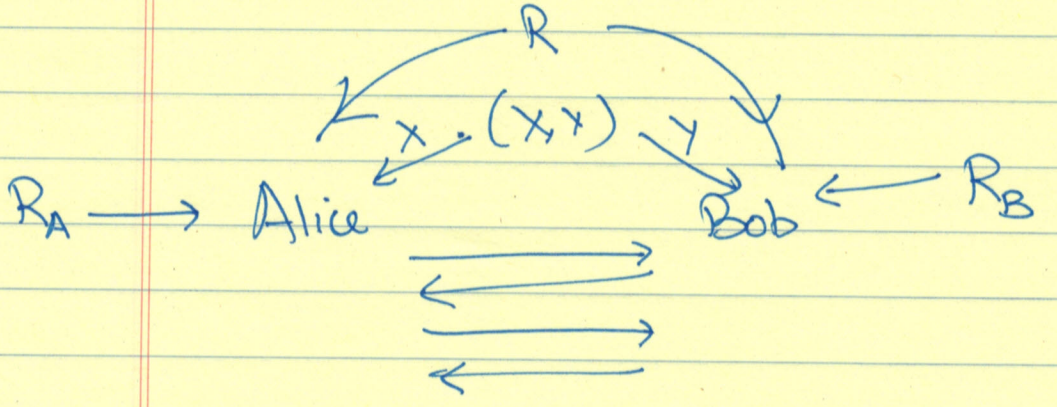
- Information-theoretic measure bounding communication complexity.

- $IC_\mu(f, \pi) \triangleq I((X,Y); \pi)$ $\quad [(X,Y) \sim \mu]$

$$IC_\mu(f) \triangleq \min_{\pi \mid \pi \text{ solves } f} \left(IC_\mu(f, \pi) \right)$$

"Information learned by observer about X, Y from π"

- More carefully.



$\pi = \pi(X, Y, R, R_A, R_B) \ldots$

$IC_\mu = I((X,Y); \pi | R)$ [condition on R; R_A, R_B might reduce information]

Example

- $AND(X,Y) = X \wedge Y$ $\quad X, Y \in \{0,1\}$; μ = uniform.
- Naive Protocol: π_{naive}

$A \xrightarrow{X} B$

$A \xleftarrow{X \wedge Y} B$

$$IC(\pi_{naive}) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 2 = \frac{3}{2}$$

- Better Protocol: t-rounds

in first $t-1$ rounds

- if Alice has 1 sends 1
- if Alice has 0 send 1 w.p. $1-\delta$, 0 w.p. δ
- same with Bob.
- if either player outputs 0, stop & output 0.

else in final round $A \xrightarrow{X} B$, $A \xleftarrow{X \wedge Y} B$.

- $IC \leq \frac{3}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot 2 = \frac{5}{4}$.

if either player has 0 learn one of the bits, but not both.

What distribution to use for DISJ?

$\mathcal{U}$: (1) Pick $Z \in \{0,1\}^n$ unif.

(2) for $i = 1$ to n do

if $Z_i = 0$ $\quad X_i = 0$ & $Y_i \sim \text{Bern}(1/2)$

if $Z_i = 1$ $\quad X_i \sim \text{Bern}(1/2)$, $Y_i = 0$.

→ Resulting dist = ~~(X,Y)~~ $\mathcal{U}$.

Funny: $\Pi = 0$ is always correct!

Catch: will want Π correct on every (X,Y) even those not in support of $\mathcal{U}$!

~~will show~~

Define $CIC_n \triangleq I(XY; \Pi \mid Z)$

(1) $CIC_n \geq n \cdot CIC_1$

(2) $CIC_1 = \Omega(1)$.

(1) $I((XY);\Pi|Z) \geq \sum_{i=1}^{n} I((X_i,Y_i);\Pi|Z)$ [Standard]

(2) $I((X_i,Y_i);\Pi|Z) \geq CIC_1 \triangleq \min_{\tilde{\Pi}} I(X_1,Y_1;\tilde{\Pi};Z_1)$

[Simulation].

(1) $I(XY;\Pi|Z) = H(XY|Z) - H(XY|\Pi,Z)$

- $H(X,Y|Z) = \sum_{i=1}^{n} H((X_i,Y_i)|Z, X_{<i}, Y_{<i})$

$= \sum_{i=1}^{n} H((X_i,Y_i)|Z)$ s.t. $(X_i,Y_i) - Z - (X_{<i},Y_{<i})$

- $H(XY|\Pi,Z) = \sum_{i=1}^{n} H((X_i,Y_i)|\Pi,Z,(X_{<i},Y_{<i}))$

$\leq \sum_{i=1}^{n} H(X_i,Y_i|\Pi,Z)$ [conditioning ...]

(1) follows.

(2) $\tilde{\Pi}$ simulates Π ...

$\uparrow$ needs

(X_1,Y_1) $(X,Y) \sim \mu^n$ → generate $Z_2 \cdots Z_n$ using common randomness

$X_2 \cdots X_n$

$Y_2 \cdots Y_n$ using private randomness.

now simulate Π.

- Int learned about X_1,Y_1 is int about X_1,Y_1 in $\Pi|Z$