CS & IT: CS229r

3/~~#~~/2019

LECTURE 12

TODAY

SET DISJOINTNESS

See also notes for L10, L11

1. INFORMATION COMPLEXITY.
2. DISJOINTNESS
3. ~~PINSKER +~~ HELLINGER DISTANCE

DISJOINTNESS

Alice $X \in \{0,1\}^n$ Bob $Y \in \{0,1\}^n$

$$\mathrm{DISJ}^n(X,Y) = 1 \text{ iff } \exists i \text{ s.t. } X_i = Y_i = 1.$$

Challenge

- Hardness needs distributions where $X \underset{\text{is not}}{\perp} Y$.
- Exercise: Prove that if $\mu = \mu_X \times \mu_Y$ then $\exists$ protocol with ~~expected~~ comm. $\tilde{O}(\sqrt{n})$. & error $\leq \epsilon$.

- Today: "Information Complexity" Approach

Warning: Distribution ✓

But not distributional lower bounds.

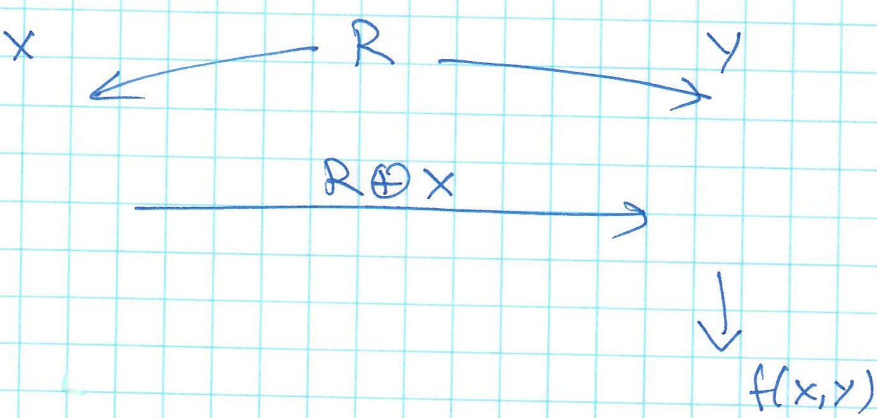
Given problem ($f = \mathrm{DISJ}^n$), consider randomized ϵ-error protocol Π; & distribution μ on inputs (X, Y)

Information Complexity of Π wrt μ is

$$IC_\mu(\Pi) \triangleq I((X,Y); \Pi) \quad \text{when} \quad (X,Y) \sim \mu$$

if $\#\text{bits}(\Pi) \le k \Rightarrow IC_\mu(\Pi) \le k \Rightarrow$ lowerbounds on IC are what we seek

Warnings: Randomness:



$IC = ?$ should

$$I((X\,Y); R \oplus X) = 0 \,!$$

Lesson: Should condition on R

$$IC_\mu(\Pi) = I((X,Y); \Pi \mid R) \;?$$

shared randomness.

Private Randomness?

Should be usable to reduce information content!

Example: $IC_{unif}(AND)$

$$\left[IC_\mu(f) \triangleq \min_{\Pi : \Pi \ \epsilon\text{-competent}} \{ IC_\mu(\Pi) \} \right]$$

Naive Protocol:

$$\text{Alice} \xrightarrow{X} \text{Bob}$$
$$\text{Alice} \xleftarrow{X \wedge Y} \text{Bob}$$

$$IC(\text{Naive}) = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 2 = \frac{3}{2}$$

Sophisticated Protocol: "continuous time version"

- if $X=0$ Alice sends X to Bob at random time $t \in [0,1]$ (unless Bob speaks before).
- if $X=1$ Alice sends X to Bob at time $t=1$ (unless Bob speaks before).

Similarly for Bob.

$$IC(\text{Soph}) = \frac{1}{4} \cdot 2 + \frac{3}{4} \cdot 1 = \frac{5}{4}.$$

Want to Prove $IC(DISJ^n) = \Omega(n)$

On what μ?

μ is a dist on (X, Y, Z) : $X, Y, Z \in \{0,1\}^n$

- sampled as follows:
  - $Z \sim \mathrm{Unif}(\{0,1\}^n)$
  - for $i = 1$ to n

    if $Z_i = 0$ then $X_i = 0$ $Y_i \sim \mathrm{Unif}(\{0,1\})$

    if $Z_i = 1$ then $X_i \sim \mathrm{Unif}(\{0,1\})$, $Y_i = 0$

- $D_{\mu,0}(DISJ^n) = 0$! [answer always 0].

- But perfect for us ... will see.

Want to Bound $IC_\mu(DISJ^n)$.

But will lower bound $\underbrace{I((XY); \Pi \mid Z, R)}$ $\leftarrow CIC_\mu(DISJ^n)$

(for protocol Π with public randomness R).

Claims: (1) $CIC(DISJ^n) \geq n \cdot CIC(DISJ^1)$ [TODAY]

(2) $CIC(DISJ^1) = \Omega(1)$ [Not Trivial !!]

$CIC(DISJ^n) \triangleq I((X,Y);\Pi \mid Z,R)$

1.1 $\quad I((X,Y);\Pi \mid Z,R) \geq \sum_{i=1}^{n} I((X_i,Y_i);\Pi \mid Z,R)$

[Simple Inf. Th.]

1.2 $\quad I((X_i,Y_i);\Pi \mid Z,R) \geq CIC(DISJ^1)$

$= \underbrace{I((X',Y');\Pi' \mid Z',R')}_{1 \text{ bit } X',Y',Z'}$

1.1 $\quad I((X,Y);\Pi \mid Z,R) = H((X,Y) \mid Z,R) - H((X,Y) \mid \Pi,Z,R)$

$- H((X,Y) \mid Z,R) = \sum_{i=1}^{n} H((X_i,Y_i) \mid Z,R) = \sum_{i=1}^{n} H((X_i,Y_i) \mid Z_i)$

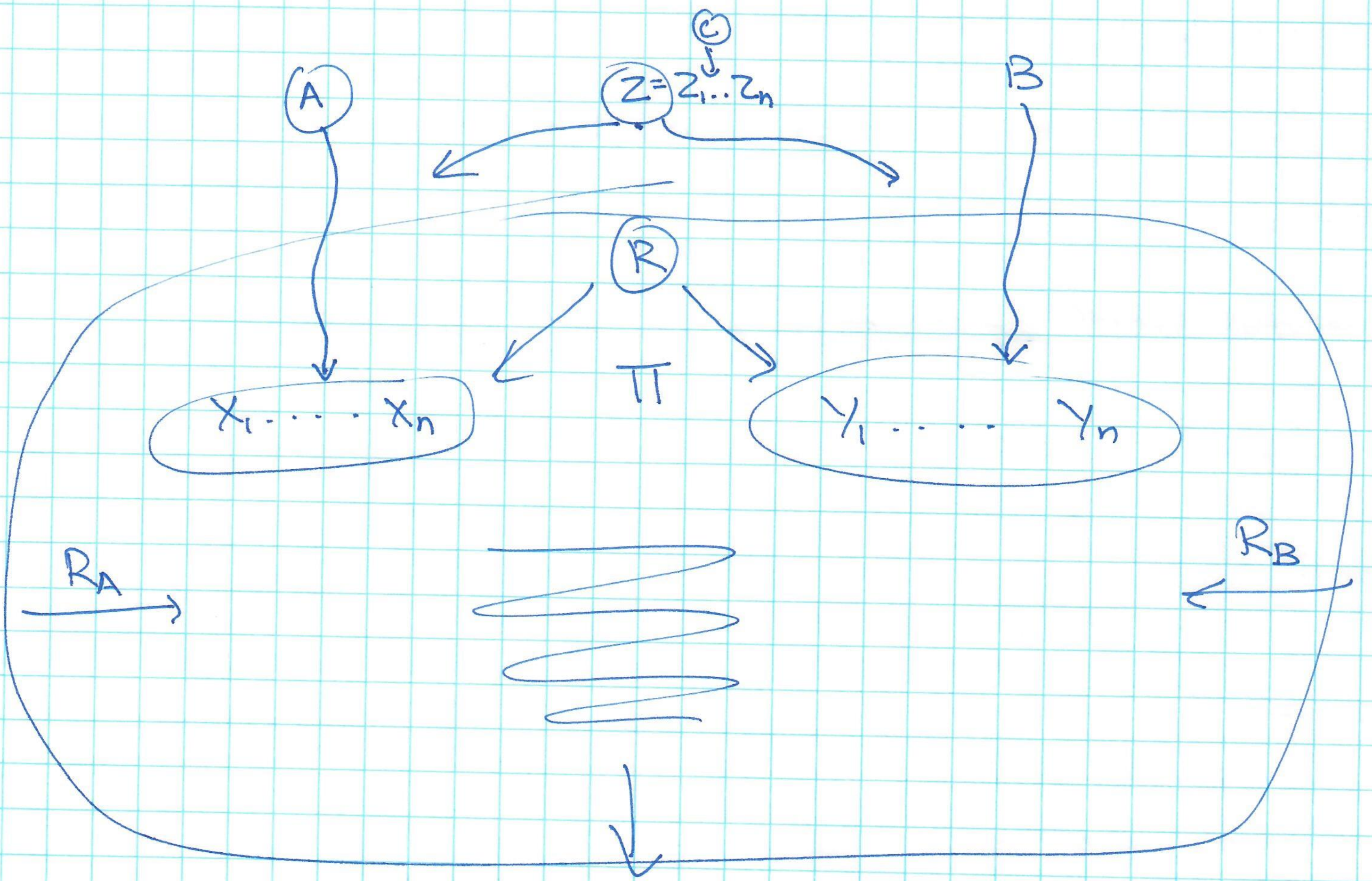
$- H((X,Y) \mid \Pi,Z,R) = \sum_{i=1}^{n} H((X_i,Y_i) \mid \Pi,Z,R,(X,Y)_{<i})$

$\leq \sum_{i=1}^{n} H((X_i,Y_i) \mid (\Pi,Z,R))$

$\boxtimes$

1.2 Non-Trivial

- Need to take protocol Π that reveals little about (X_i, Y_i) while computing DISJ
- Convert to protocol Π' that reveals little about A, B while computing $A \wedge B$.



$\text{DISJ}(X_1 \ldots X_n, Y_1 \ldots Y_n) = \text{AND}(A, B)$?

get lower bound on $I((X_i, Y_i) \mid \Pi, R, Z) \leftarrow$

need lower bound on $I((A, B) \mid C, \Pi, \tilde{R}) \leftarrow$

are these same?