LECTURE 12

Note Title 3/2/2016

TODAY

- (Internal) Information Complexity
- Direct Sum Problems
- Lower bound on direct sum complexity

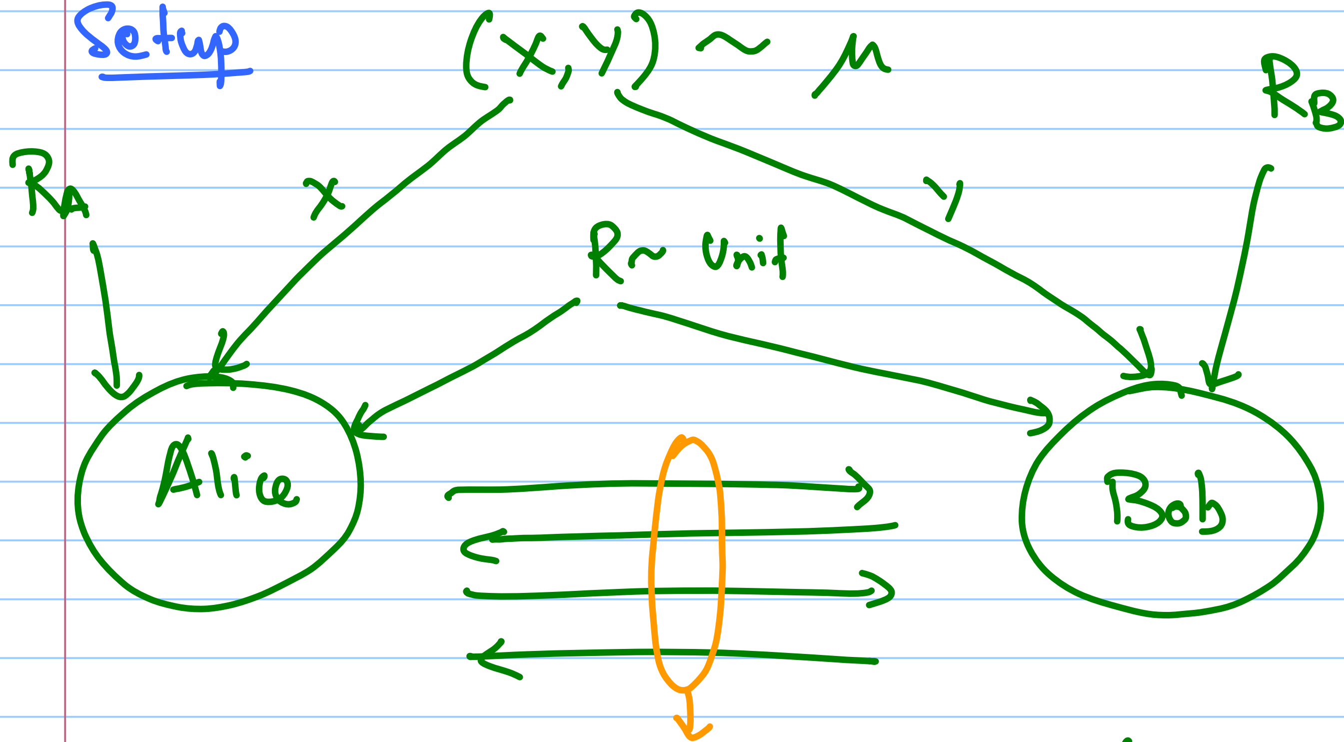
References

[Barak, Braverman, Chen, Rao]

[Braverman, Rao]

Recall (External) Information Complexity

Setup



$$\Pi = \Pi(X,Y) = \Pi(X,Y,R,R_A,R_B)$$

[Π deterministic function of (X,Y,R,R_A,R_B)]

$$\boxed{IC^{ext}_{\mu}(\Pi) \triangleq I(XY;\Pi \mid R)}$$

External Information Cost ≡ What an observer learns about Alice & Bob's input from the interaction.

-

Internal Information Cost

Correspondingly: (Sum of) What the players learn about each other's inputs.

$$\boxed{IC^{int}_{\mu}(\Pi) \triangleq I(X;\Pi \mid Y,R) + I(Y;\Pi \mid X,R)}$$

Fact: $\forall \Pi, \mu$

$$IC^{int}_{\mu}(\Pi) \leq IC^{ext}_{\mu}(\Pi) \leq CC_{\mu}(\Pi)$$

Proof: 2^{nd} Inequality already covered in previous lectures.

- Wish to show

$$I(XY;\Pi \mid R) \geq I(X;\Pi \mid Y,R) + I(Y;\Pi \mid X,R)$$

- Let $\Pi = \Pi_1 \ldots \Pi_\ell$

Lets ignore R (holds $\forall R=r$)

.

- $I(XY;\Pi) = I(\Pi; XY)$

$$= \sum_{i=1}^{\ell} I(\Pi_i ; XY \mid \Pi_1 .. \Pi_{i-1})$$

Similarly

$$I(X;\Pi|Y) = \sum_{i=1}^{\ell} I(\Pi_i ; X \mid Y \Pi_1 .. \Pi_{i-1})$$

etc.

Claim

$$I(\Pi_i ; XY \mid \Pi_1 ... \Pi_{i-1}) \geq I(\Pi_i ; X \mid Y\Pi_1 .. \Pi_{i-1}) + I(\Pi_i ; Y \mid X\Pi_1 .. \Pi_{i-1})$$

(Claim $\Rightarrow$ Fact is obvious)

Proof of Claim (Assume wlog Alice speaks)

- $I(\Pi_i ; XY \mid \Pi_{<i}) = I(\Pi_i ; X \mid \Pi_{<i}) + I(\Pi_i ; Y \mid \Pi_{<i}, X)$

- Suffices to show

$$I(\Pi_i ; X \mid \Pi_{<i}) \geq I(\Pi_i ; X \mid \Pi_{<i}, Y)$$

But RHS = 0 (since Bob speaks and so $X \to Y \to \Pi_i$)

(informally Bob can't learn anything about X when he speaks, but observer can).

$\boxtimes$

Why study Internal Information Cost?

Quantity "tensorizes"

Recall

$$IC_{\mu,\epsilon}(f) \triangleq \min_{\pi} \{ IC_{\mu}(\pi) \}$$

s.t. $err_{\mu}(\pi, f) \leq \epsilon$

n-fold direct sum of f

$$f^{\otimes n}(x_1 x_2 \ldots x_n\ y_1 \ldots y_n) = (f(x_1,y_1) \ldots f(x_n, y_n))$$

- Trivially

$$CC_{\mu^n,\ 1-(1-\epsilon)^n}(f^{\otimes n}) \leq n \cdot CC_{\mu,\epsilon}(f)$$

(Repeat Π on n problem instances)

- Can we do better?
  for some f?
- For long... open

Results

① [BBCR]

$$CC_{\mu^n,\epsilon}(f^{\otimes n}) \geq \tilde{\Omega}(CC_{\mu}(f)\cdot\sqrt{n})$$

② [BR]

$$\lim_{n\to\infty} \frac{CC_{\mu^n,\epsilon}(f^{\otimes n})}{n} = IC_{\mu,\epsilon}(f)$$

(fine point: will redefine
$CC_{\mu^n,\epsilon}(f^{\otimes n})$ for ②)

Central Ingredients [BBCR]

1. Rough Tensorization of Information Complexity

$$IC_{\mu^n, 0}(f^{\otimes n}) = n \cdot IC_{\mu, 0}(f)$$

2. Embedding $f \to f^{\otimes n}$ while incurring $\frac{1}{n}$ of Information cost.

3. Compressing protocols with low information cost.

Some Lemmas

Lemma 1: if $f^{\otimes n}$ has protocol with communication C & (internal) information I then f has protocol with communication C & information I/n (Tensorization + Embedding)

Lemma 2: if g has protocol with comm. C & information I then g has protocol with communication $O(\sqrt{CI}\log C)$. (Compression)

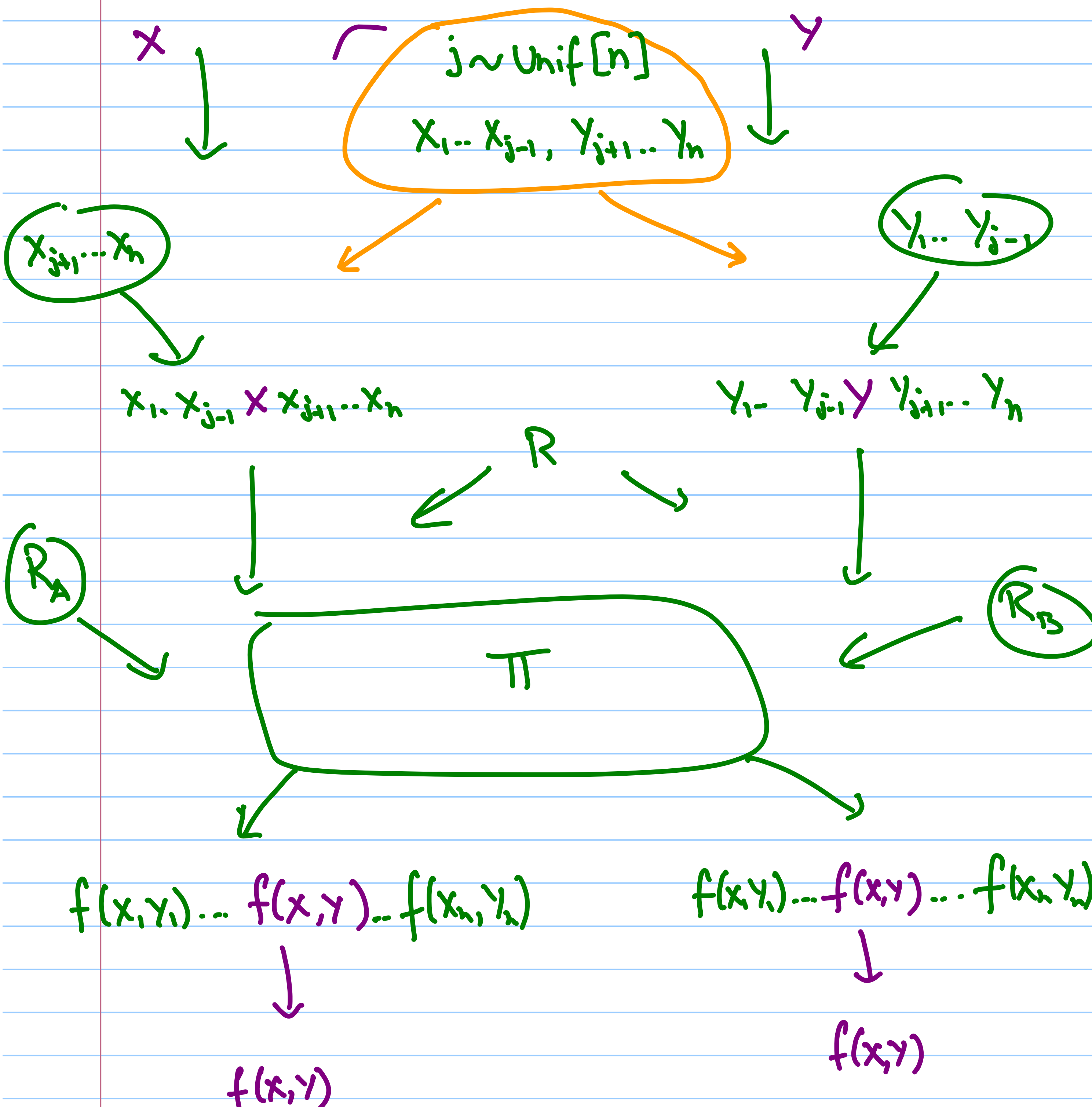
(Lemma 1 + Lemma 2 immediately imply [BBCR])

Proof of Lemma 1

Embedding Challenge

- Want to compute $f(x,y)$
- have protocol for $(f(x_1,y_1) \dots f(x_n,y_n))$
- Need to
  - map inputs $\begin{array}{l} x \to x_1 \dots x_n \\ y \to y_1 \dots y_n \end{array}$
  - map outputs $$\begin{array}{c} (f(x_1,y_1) \dots f(x_n,y_n)) \\ \downarrow \\ f(x,y) \end{array}$$
  - reduce (information) cost!
- Idea: (from disjointness)

Embedding



- Clearly: Inputs are right, outputs are right
- Does information complexity reduce?
- Why sample some things publicly & others privately

$$I(X;\Pi \mid j, X_1 \ldots X_{j-1} Y_{j+1} \ldots Y_n, Y)$$

$$\overset{?}{\leq} \quad \frac{1}{n} I(X_1 \ldots X_n ; \Pi \mid Y_1 \ldots Y_n)$$

Compare

$$\frac{1}{n} \sum_{i=1}^{n} I(X_i ; \Pi \mid X_1 \ldots X_{i-1}, Y_1 \ldots Y_n)$$

$$I(X_j ; \Pi \mid j, X_1 \ldots X_{j-1}, Y_1 \ldots Y_n)$$

extra $Y_1 \ldots Y_{j-1}$

- Is $I(X_j ; \Pi \mid j, X_1 \ldots X_{j-1} Y_j Y_{j+1} \ldots Y_n)$

$$\leq I(X_j ; \Pi \mid j\, X_1 \ldots X_{j-1}\, Y_1 \ldots Y_n) \quad ?$$

What did Bob learn about X_j from the protocol

What did Bob learn about X_j from protocol + his private randomness.

(both equal)

Lemma 2 (proof on Tuesday)

Musings

(1) Definition of Information Cost vs. Public Randomness

[Our definition] : $I(XY; \Pi \mid R)$

[BBCR definition] : $I(XY; \Pi R)$

Prop: Two definitions equal, since
$XY \perp R$

Proof: $I(XY; \Pi \mid R) = H(XY \mid R) - H(XY \mid \Pi R)$

$= H(XY) - H(XY \mid \Pi R) \quad (XY \perp R)$

$= I(XY \mid \Pi R)$

—— x ——

② Internal Cost & Private Randomness:

What does Bob learn from protocol about X?

actually: $I(X;\Pi \mid Y, R_B, R)$

our defn: $I(X;\Pi \mid Y, R)$

Prop: Both same

Proof: Note $R_B \longrightarrow (\Pi, Y) \longrightarrow X$

& $R_B \to Y \to X$

So $I(X;\Pi \mid Y, R_B)$

$$= H(X \mid Y, R_B) - H(X \mid Y, R_B, \Pi)$$

$$\qquad \| \qquad\qquad\qquad\qquad \|$$

$$= H(X \mid Y) - H(X \mid Y, \Pi)$$

(3) Embedding: Why not simpler choices?

Idea 1: Use private randomness to sample

$$X_{-j}, Y_{-j}$$

· But X_i, Y_i need to be correlated!

(works for product distributions though)

Idea 2: Use public randomness.

- Proof doesn't work ☹
- Actually Lemma is false!
- e.g.

$$\Pi(X_1 \ldots X_n, Y_1 \ldots Y_n): \quad A \xrightarrow{\oplus X_i} B$$

(x_i, y_i bits)

$$I(X ; \Pi \mid Y) \leq 1$$

$$I(X_j ; \Pi \mid X_{-j}, Y_{-j}) = 1 \quad (\text{not } \tfrac{1}{n})$$