Outline

- set disjointness problem
- information complexity of a protocol
- IC $\leq$ CC
- choice of distribution + conditional information complexity
- CIC $\leq$ IC
- $CIC^n \geq n \cdot CIC^1$
- $CIC^1 = \Omega(1)$

Set Disjointness Problem

Alice, Bob respectively have $X, Y \in \{0,1\}^n$, want to compute $DISJ(X,Y)$

$$DISJ(X,Y) = \bigvee_{i=1}^{n} (X_i \wedge Y_i)$$
$$= \begin{cases} 1 & \text{if } \exists i \text{ s.t. } X_i = Y_i = 1 \\ 0 & \text{o.w.} \end{cases}$$

If X is characteristic vector of set S, Y is characteristic vector of T, $DISJ(X,Y)$ computes if the intersection of S + T is nonempty, i.e. whether the sets are disjoint or not.

Goal: lower bound the communication complexity (CC) for a randomized protocol Π for computing $DISJ(X,Y)$ using information theory.

Information Complexity

Definitions/Preliminaries

- $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$
- μ is a distribution on $\{0,1\}^n \times \{0,1\}^n$
- ϵ is an error parameter
- Π is a correct protocol for f ($\Pi(X,Y)$ outputs $f(X,Y)$ $\forall X, Y$)
- $\Pi(X, Y, R, R_A, R_B)$ is the transcript of protocol Π with inputs X + Y, private randomness R_A + R_B, and public randomness R. Notated as Π.

Def: the information cost $(IC^{\Pi}_{\mu,\epsilon}(f))$ of Π wrt μ is $I(X, Y; \Pi | R)$; intuitively this is the amount of information learned about the inputs X, Y from the transcript

Def: the ϵ-error information cost $(IC_{\mu,\epsilon}(f))$ of f wrt μ is the minimum information cost of an ϵ-error protocol Π for f wrt μ:

$$IC_{\mu,\epsilon}(f) \triangleq \min_{\Pi} \{ IC^{\Pi}_{\mu,\epsilon}(f) \}$$

Ex. protocol with nontrivial information complexity : 1-bit AND

setup : $X, Y \in \{0,1\}$, $f(X,Y) = X \wedge Y$

protocol : parameters $k >> \frac{1}{\delta}$, $\delta \to 0$

repeat k times:
- $A \to B$ send 1 w.p. $1-\delta$, X w.p. δ
- $B \to A$ send 1 w.p. $1-\delta$, Y w.p. δ
- if either bit 0, stop + output 0

else output 1

Correctness : protocol incorrect w.p. $\leq e^{-\delta k}$

Information complexity < 2 since protocol ends w/ either X or Y unknown

Lemma : for any μ and $\epsilon > 0$, $CC_\epsilon(f) \geq IC_{\mu,\epsilon}(f)$

Pf : Let Π^* be a protocol that solves f with error probability $\leq \epsilon$

Recall $CC_\epsilon(\Pi) = |\Pi|$ is the max length of $\Pi(X,Y,R,R_A,R_B)$ over all inputs X, Y.

$$CC_\epsilon(f) = |\Pi^*| \geq H(\Pi^*) \geq I(X,Y;\Pi^*|R) = IC_{\mu,\epsilon}(f)$$

□

Goal : lower bound CC(DISJ) via the information complexity of DISJ.

Thm : $IC_{\mu,\epsilon}(DISJ) = \Omega(n)$

Proof strategy : ① $IC(DISJ^n) \geq n \cdot IC(DISJ')$ ("Direct Sum")

② $IC(DISJ') = \Omega(1)$

The Choice of Distribution and Conditional Information Complexity

Want to show $IC^n \geq n \cdot IC'$ but hindered by fact that distribution μ of inputs (X,Y) is not a product distribution. To get around this, use auxiliary random variable $Z \sim Unif(\{0,1\}^n)$. Then construct a new distribution η^n in following way:

If $Z_i = 0$, $X_i = 0$ and $Y_i \sim Unif(\{0,1\})$

If $Z_i = 1$, $Y_i = 0$ and $X_i \sim Unif(\{0,1\})$

η^n is the joint distribution (X,Y,Z).

This new distribution has the following properties:
- $\forall\, x,y \in$ support of η^n, $DISJ(x,y) = 0$
- $\forall\, Z \in \{0,1\}^n$, $X \perp Y \mid Z$

Def : the conditional information cost ($CIC^{\Pi}_{\eta,\epsilon}(f)$) of Π wrt η^n is $I(X,Y;\Pi|Z,R)$

Def : the conditional information complexity ($CIC_{\eta,\epsilon}(f)$) of f wrt η^n is the minimal conditional information cost of a protocol that solves f:

$$CIC_{\eta,\epsilon}(f) = \min_{\Pi} \{ CIC^{\Pi}_{\eta,\epsilon}(f) \}$$

Lemma : $IC_{\mu,\epsilon}(f) \geq CIC_{\eta,\epsilon}(f)$ where $\eta^n | Z = \mu$

Pf : Note that a protocol Π for f is independent of Z given X, Y. Then,

$$IC_{\mu,\epsilon}(f) = \underbrace{I(X,Y;\Pi)}_{H(\Pi) - H(\Pi|X,Y)} \geq \underbrace{I(X,Y;\Pi|Z)}_{H(\Pi|Z) - H(\Pi|X,Y,Z)} = CIC_{\eta,\epsilon}(f) \quad \text{(dropping conditioning on } R)$$

$$H(\Pi|X,Y) = H(\Pi|X,Y,Z)$$

$$H(\Pi) \geq H(\Pi|Z)$$

□

Direct Sum for CIC: Proof of ①

Want to show $CIC^n \geq n \cdot CIC'$. Divide into two parts:

Ⓐ $CIC^n = I(X,Y;\Pi|Z) \geq \sum_{i=1}^{n} I(X_i,Y_i;\Pi|Z)$

Ⓑ $I(X_i,Y_i;\Pi|Z) \geq CIC_{\zeta,\epsilon}(DISJ')$ where $\eta = \zeta^n$

Pf of A: $I(X,Y;\Pi|Z) = H(X,Y|Z) - H(X,Y|\Pi,Z)$

$$H(X,Y|Z) = \sum_{i=1}^{n} H(X_i,Y_i|Z,X_1,Y_1,\dots,X_{i-1},Y_{i-1}) \quad \text{(chain rule)}$$

$$= \sum_{i=1}^{n} H(X_i,Y_i|Z) \quad (X_i,Y_i \perp \{X_j,Y_j\}_{j\neq i})$$

$$H(X,Y|\Pi,Z) = \sum_{i=1}^{n} H(X_i,Y_i|Z,\Pi,X_1,Y_1,\dots,X_{i-1},Y_{i-1}) \leq \sum_{i=1}^{n} H(X_i,Y_i|Z,\Pi) \quad \text{(conditionally reduces entropy)}$$

□

Next time: Proof of Ⓑ and ② to complete proof of the theorem.