Monday, February 22, 2016 11:42 AM

Information Complexity & Set Disjointness

- Set Disjointness Problem
- Information Complexity Definition
- Communication $\geq$ Information
- The Distribution μ_n
- $IC(Disj^n_{\mu_n}) \geq n \cdot IC(Disj^1_{\mu_1})$

- $IC(Disj^n_{\mu^n}) \geq n \cdot IC(Disj^1_{\mu^1})$

- $IC(Disj^1_{\mu^1}) = \Omega(1)$

Disjointness Problem

(really dis-dis-jointness?)

$$Disj^n(x,y) = \bigvee_{i=1}^{n} (x_i \wedge y_i)$$

$$= \exists i \text{ s.t. } x_i = y_i = 1$$

$\int S$

= if x is char. vector of S
& y is char. vector of T
then "is $S \cap T \neq \phi$?"

Information Complexity

$IC_{\mu,\epsilon}(f)$

- $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1,?\}$

  bnl. on $\{0,1\}^n \times \{0,1\}^n$

- μ distribution on $\{0,1\}^n \times \{0,1\}^n$

- ϵ : error parameter

- Let Π be a correct protocol
  ($\Pi(x,y)$ outputs $f(x,y)$ $\forall\, x,y$)

- Notation: $\Pi \triangleq$ transcript of protocol
  (so $\Pi = \Pi(x,y,R,R_A,R_B)$)

  R: Common

  R_A, R_B: private randomness

randomness

$$- \underbrace{IC}^{\pi}_{\mu,\epsilon}(f) = \underbrace{I}(XY;\pi)$$

Information Complexity

Mutual Information

$$- IC_{\mu,\epsilon}(f) \triangleq \min_{\pi} \left\{ \underbrace{IC}^{\pi}_{\mu,\epsilon}(f) \right\}$$

P_1 1 with non-trivial Information Complexity

Protocol with [illegible]

1-bit AND : $x, y \in \{0,1\}$

$f(x,y) = x \wedge y$

Protocol: Parameters $R \gg \frac{1}{\delta}$, $\delta \to 0$

Repeat R times:

- $A \to B$: Send 1 w.p. $1-\delta$
  Send x w.p. δ
- $B \to A$: Send 1 w.p. $1-\delta$
  Send y w.p. δ

$\frac{1}{2p+\delta}$

(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 with either x or y unknown.

(can do formal analysis)

V

Lemma:

$$CC_\epsilon(f) \geq IC_{\mu,\epsilon}(f)$$

↑ ϵ-error communication complexity

Proof: "Trivial"

- Let Π solve f with error prob. $\leq \epsilon$
- $CC_\epsilon(f) = |\Pi| \geq H(\Pi)$ ⊠
- $IC_{\mu,\epsilon}(f) = I(XY;\Pi) \leq H(\Pi)$

———— ∞ ————

Corollary: $\forall f, \forall \mu \sim (X, Y, Z)$

$$CC_\epsilon(f) \geq IC_{\mu|Z, \epsilon}(f)$$

- $\mu|Z$ = μ conditioned on Z.
- Proof: $\forall z$ we have

$$CC_\epsilon(f) \geq IC_{\mu|_z, \epsilon}(f)$$

$\therefore$ so $CC_\epsilon(f) \geq IC_{\mu|Z, \epsilon}(f)$

The Distribution

- $(X, Y, Z) \sim \mu = \mu_n$ sampled as follows

- Independently pick

$$\tilde{X} \sim \text{Unif}(\{0,1\}^n)$$
$$\tilde{Y} \sim \text{Unif}(\{0,1\}^n)$$
$$Z \sim \text{Unif}(\{0,1\}^n)$$

- Set $X = \tilde{X} \wedge Z$

↑ coordinate wise - and

$$Y = \bar{Y} \wedge Z$$

↑ negation of Z

Features of μ

(1) $\forall (x,y) \in$ support of μ

$$\text{Disj}(x,y) = 0$$

(2) $\forall z \in \{0,1\}^n$

$\mu|_z$ satisfies $X \perp Z$

Main Theorem $IC_{\mu_n|2,\epsilon}(DISJ^n) = \Omega(n)$

Lemma $(X,Y,Z) \sim \mu_n$

$$I(XY;\Pi \mid Z) = \Omega(n)$$

Lemma 1

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

Lemma 2

$$I(X_i, Y_i; \Pi \mid Z) \geq IC_{\mu_1, \epsilon}(\text{DISJ}')$$

↑ 1-bit disjointness

Lemma 3

$$IC_{\mu_1, \epsilon}(\text{DISJ}') > 0$$

Obviously Lemma [illegible]

$\Rightarrow$ Lemma $\Rightarrow$ Main Theorem

Rest of lecture(s): Proof of Lemma 1, Lemma 2, Lemma 3.

Proof of Lemma 1

Straight forward manipulation / Chain Rule

$$I(XY;\Pi|Z) = \underbrace{H(XY|Z)}_{①} - \underbrace{H(XY|\Pi,Z)}_{②}$$

① : $H(XY|Z) = \sum_{i=1}^{n} H(X_iY_i \mid Z X_1Y_1 \cdots X_{i-1}Y_{i-1})$

(Chain Rule)

$= \sum_{i=1}^{n} H(X_iY_i|Z)$

$(X_iY_i \perp \{X_jY_j\}_{j \neq i})$

② $H(XY|\Pi,Z) = \sum_{i=1}^{n} H(X_iY_i \mid Z\Pi, X_1Y_1 \cdots X_{i-1}Y_{i-1})$

(Chain Rule)

)

$\leq \sum_{i=1}^{n} H(X_i, \pi \mid$ —

(Conditioning Reduces Entropy)

Putting above together

$$I(XY; \pi \mid Z) \geq \sum_{i=1}^{n} I(X_i Y_i; \pi \mid Z)$$

—— ∅ ——

Proof of Lemma 2