LECTURE 8

Friday, February 19, 2016
9:12 PM

TODAY

COMMUNICATION COMPLEXITY

- Model
- Example: Equality testing
- Det. Lower bound
- Prob. Communication complexity
- Discrepancy Lower Bound
- Information Theoretic L.B. - Indexing

Model

Informally:

- Alice has input $x \in \{0,1\}^n$
- Bob has $y \in \{0,1\}^n$
- Want to compute joint function $f(x,y)$

$f(x,y)$ of communication

- Question how many bits needed?

Example

$f(x,y) = EQ(x,y) = 1$ if $x = y$

$= 0$ o.w.

Naive Protocol

- Alice sends $x \longrightarrow$ Bob

Bob sends 1 if $x = y$;

0 o.w.

- Complexity = $n+1$
- Fact: All functions have complexity $\leq n+1$
- Which functions have complexity $\Omega(n)$?

– Can complexity of EQ? be smaller?

Model Formally

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

  ↑ sometimes undefined

- Solution = Protocol = $\Pi = (\pi_1 \ldots \pi_k ; g_A, g_B)$

  $\pi_i = (z_i \in \{x, y\}$ (who speaks)

  $f_i(z_i, b_1 .. b_{i-1})$ (& what they say))

- Correctness: If $b_i = f_i(z_i, b_1 .. b_{i-1}) \quad \forall i$

  & then $g_A(x, b_1 .. b_k) = g_B(y, b_1 .. b_k) = f(x, y)$

  $(\forall x, y)$

Complexity: $k \triangleq$ # bits transmitted

Randomized Complexity

Private Randomness:

- Alice/Bob toss coins privately & use that to determine which bits to send.

- Want

$$\forall x, y \quad \Pr_{\$}\left[g_A(\ ) \neq f(x,y) \text{ or } g_B(\ ) \neq f(x,y) \right] \leq \epsilon$$

Public Randomness

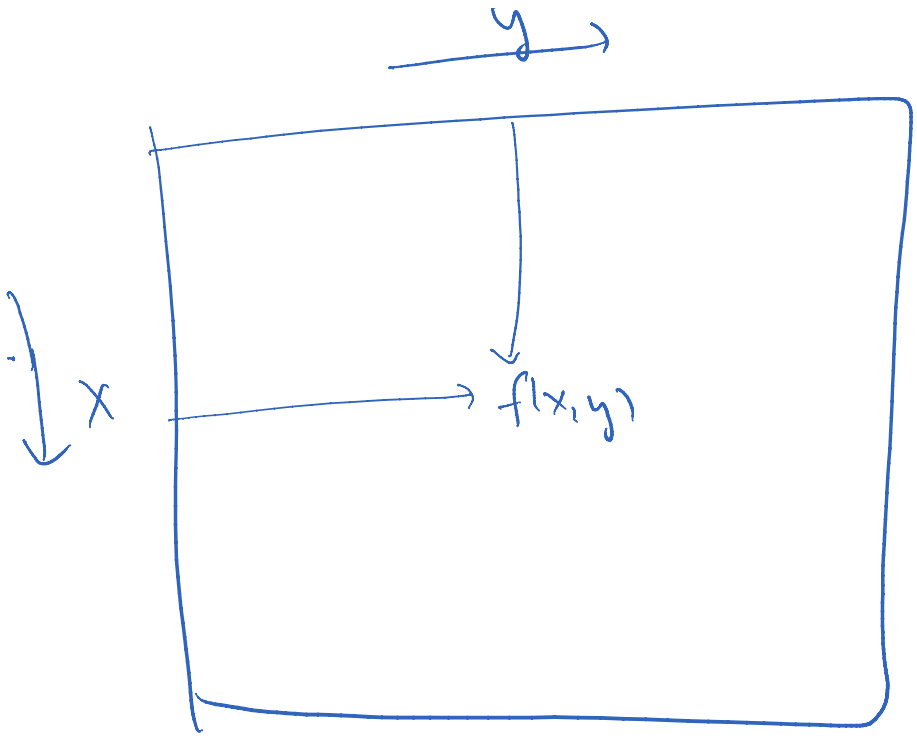
- Alice, Bob $\leftarrow R$

want $\forall x, y$

$$\Pr_{R}\left[g_A(\ ) \neq f(x,y) \text{ or } g_B(\ ) \neq f(x,y) \right] \leq \epsilon$$

Deterministic Lower Bound on EQ

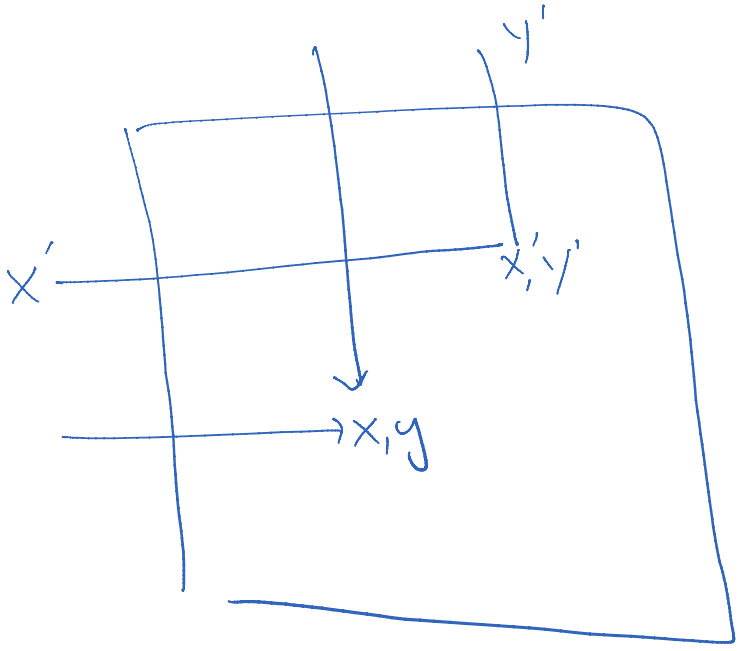
Often think about Comm. Matrix M_f



What does M_f look like combinatorially / linear algebraically

---

Claim 1 (Rectangle Property)



Protocol transcript = $t(x,y) = (b_1, \ldots b_k)$

---

if $t(x,y) = t(x',y')$

then $t(x',y) = t(x,y') = t(x,y)$

Consequence

if $cc(f) \leq k$ then M_f can be written as union of 2^k rectangles each of which is constant wrt f.

$\Rightarrow$

$\text{Rank}(M_f) \leq 2^k$

Theorem [1/40]: $cc(EQ) \geq n$

- $M_{EQ} = 2^n \times 2^n$ Identity matrix

$\ldots \quad 2^n$

$\cdots_{EQ}$

- $\text{Rank}(M_{EQ}) = 2^n$

Randomized Complexity of EQ

Tool: Error correcting code

Claim: $\exists\ E : \{0,1\}^n \to \{0,1\}^{2n}$

s.t. $\forall\ x, y$ $E(x), E(y)$ differ in 10% of coordinates.

Proof omitted: (take my other course!)

Protocol: Alice & Bob share $i \leftarrow_U [2n]$

Given x, y

$A \to B$: $E(x)_i$

$B \to A$: 1 if $E(x)_i = E(y)_i$

- 0 o.w.

- Complexity = 2 bits
- if $x=y$ always correct
- if $x \neq y$ error $\leq 90\%$
- amplify by repeating

Can convert to private randomness with Alice picking $i \in [2n]$ & sending $i, E(x)_i$ to Bob.

Proving Lower Bounds On Randomized Communication Complexity

(1) Use distribution on inputs

$(x, y) \sim \mu(\{0,1\}^n \times \{0,1\}^n)$

- if $\exists$ randomized protocol that achieves error ϵ, then $\exists$ det. protocol that achieves error ϵ on μ.

- Prove there is no det. protocol with error ϵ on μ.

---

(2) Matrix view of distributional complexity

(2a) $f: \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$

(2b) $M_{\mu,f}(x,y) = \mu(x,y) \cdot f(x,y)$

(2c) Rectangle: $R(x,y) \in \{0,1,-1\}$ function s.t. $\exists\ S \subseteq \{0,1\}^n, T \subseteq \{0,1\}^n$ & $b \in \{1,-1\}$

s.t. $R(x,y) = 0$ if $(x,y) \notin S \times T$

$= b$ if $(x,y) \in S \times T$

(2d) Discrepancy of Rectangle R wrt (f, μ)

$$\text{Disc}_{\mu,f}(R) = \sum_{x,y} M_{\mu,f}(x,y) \cdot f(x,y)$$

(2e) Error of protocol $\Pi = \epsilon$

$$\iff \sum_{t} \text{Disc}_{\mu,f}(R_t) \geq 1 - 2\epsilon \geq \frac{1}{2}$$

[R_t = Rectangle corr. to transcript t]

$\Rightarrow \exists$ rectangle with $\text{Disc}(R) \geq 2^{-k}\left(\frac{1}{2}\right)$

(2f) $\text{Disc}(M) = \max_{\text{rectangle } R} \text{Disc}_M(R)$

(2g) Linear Algebra Upper bound on $\text{Disc}(M)$

$$Disc(M) \triangleq \max_{u \in \{0,1\}^{2^n}, v \in \{0,1\}^{2^n}} \{u^T M v\}$$

$$\leq \max_{u,v \in R^{2^n}, |u|_2, |v|_2 \leq 2^{n/2}} \{u^T M v\}$$

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

↑ largest singular value of M

PROBLEM with $\Omega(n)$ lower bound on Prob. Comm. Complexity

---

Inner Product Function $x, y \in \{0,1\}^n$

$$IP(x,y) = \prod_{i=1}^{n} (-1)^{x_i \cdot y_i}$$

- $IP(x,y) = \prod_{i=1}^{n} (-1)^{x_i \cdot y_i}$
- $\mu(x,y) = \text{Unif}(\{0,1\}^n \times \{0,1\}^n)$
- $M^n_{\mu,IP}(x,y) = \frac{\prod_{i=1}^{n} (-1)^{x_i y_i}}{4^n} = \prod_{i=1}^{n} \left[\frac{(-1)^{x_i y_i}}{4} \right]$

$$= \left(M^1_{\mu,IP} \right)^{\otimes n}$$

- $\lambda_{max}\left(M^n_{\mu,IP}\right) = \lambda_{max}\left(M^1_{\mu,IP}\right)^n$

$$M^1_{\mu,IP} = \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & -1/4 \end{bmatrix}$$

$$\lambda_{max}\left(M^1_{\mu,IP}\right) = \frac{1}{\sqrt{8}} < \frac{1}{2}$$

$$\Rightarrow \text{Disc}(M^n_{\cdot,\cdot}) \leq \left(\frac{1}{2}\right)^n \leq 2^{-n/2}$$

$$\Rightarrow \mathrm{Disc}\left(M'_{\mu,1/2}\right) \le \left(\frac{2}{\sqrt{8}}\right)^k \le \alpha$$

$$\Rightarrow k = \Omega(n) \text{ to get error} < \frac{1}{4}.$$

Information Theory in Lower Bounds

Simple Example: One-way complexity of Indexing

Problem: $X \in \{0,1\}^n$; $i \in [n]$

X → Alice

i → Bob

$f(x,i) = x_i$

Two-way Solution:

Bob → Alice : i

Alice → Bob : x_i

Complexity $= 1 + \lceil \log n \rceil$

Complexity = $1 + \lceil \log n \rceil$

One-way Problem

Only Communication allowed: Alice → Bob

Only Bob needs to output $f(x, y)$

Theorem: One-way Complexity (Indexing) = $\Omega(n)$

Proof: $\mu = \text{unif}(\{0,1\}^n) \times \text{unif}([n])$

- Let $m = m(x)$ be Alice's message to Bob.
  & $g = g(m, i)$ be Bob's output.

- $\Pr_{x,i}\left[g(m(x), i) = x_i \right] > \frac{9}{10}$ — (1)

- Let $y = y_1 \cdots y_n$ be given by $y_i = g(m(x), i)$

- (1) $\Rightarrow$ $I(X;Y) = \Omega(n)$

- But $X \rightarrow m \rightarrow Y$

$\Rightarrow I(X;Y) \leq I(m;Y) \leq |m|$

$\Rightarrow$ extra length of $m = \Omega(n)$ ☒