①

Tue 4/9

Today: Lower bounds on dist. CC.
Discrepancy
Index problem via Inf. Theory.

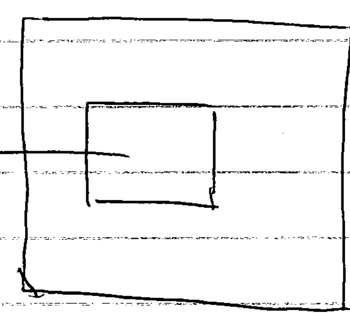
Recall: $R_\delta^{prob}(f) = \max_\mu D_\delta^\mu(f)$.

Lower bound $D_\delta^\mu(f)$ for some clever choice of μ.

Again, rectangles idea. But OK to be slightly non-monochromatic.

Discrepancy Method:

all large rectangles have nearly equal # of 0's and 1's



$\Downarrow$

The protocol has to use small rectangles

$\Downarrow$

Large C.C.

Def. $f: X \times Y \to \{0,1\}$

R = rectangle $= S \times T$, $S \subseteq X$, $T \subseteq Y$.

μ dist. on $X \times Y$.

$$\mathrm{Disc}_\mu(R, f) \triangleq \left| \Pr_{(x,y)\sim\mu}\left[(x,y)\in R, f(x,y)=0\right] - \Pr\left[(x,y)\in R, f(x,y)=1\right] \right|$$

②

$$= \left| \sum_{(x,y)\in R} (-1)^{f(x,y)} \mu(x,y) \right| .$$

$$\mathcal{D}isc_{\mu}(f) \triangleq \max_{\substack{R, \\ R \text{ rectangle}}} \mathcal{D}isc_{\mu}(R, f).$$

Ex: R monochromatic $\Rightarrow \mathcal{D}isc_{\mu}(R,f) = \mu(R)$.

saw earlier:

$$* \quad \mathcal{D}(f) \geq \log_2 \left(\frac{1}{\max_{\substack{R \\ R \text{ rectangle}}} \mu(R)} \right)$$

* Proposition: (Discrepancy Lower Bound)

$$\mathcal{D}^{\mu}_{\frac{1}{2}-\gamma}(f) \geq \log_2 \left(\frac{2\gamma}{\mathcal{D}isc_{\mu}(f)} \right).$$

Proof: Π be a protocol using c bits of communication

& error probability $\leq \frac{1}{2} - \gamma$.

We know: $\Pr\left(\Pi(x,y) = f(x,y)\right) - \Pr\left(\Pi(x,y) \neq f(x,y)\right) \geq 2\gamma$

We decompose the probability into the partition defined by Π.

(3)

$$LHS = \sum_{\substack{R_\ell \text{ of} \\ \text{protocol}}} \Big(\Pr_\mu \big[\Pi(x,y) = f(x,y) \wedge (x,y) \in R_\ell \big] - \Pr_\mu \big[\text{''} \neq \text{''} \quad \text{''} \big] \Big)$$

NB: Π is constant on R_ℓ.

$$\Rightarrow LHS \leq \sum_{R_\ell} \Big| \Pr_\mu \big(f(x,y) = 0 \wedge (x,y) \in R_\ell \big) - \Pr_\mu \big(f(x,y) = 1 \wedge (x,y) \in R_\ell \big) \Big|$$

$$= \sum_{R_\ell} \mathcal{D}isc_\mu (R_\ell, f) \leq 2^c \cdot \mathcal{D}isc_\mu (f).$$

$\square$

<u>Ex:</u> Dot product: $IP(x,y) = \langle x,y \rangle \bmod 2$.
$(x,y \in \{0,1\}^n)$

<u>Theorem:</u> $R_{1/3}(IP) = \Omega(n) \quad \left(\geq n/2 - O(1) \right)$

Suffices to show: $\mathcal{D}^\mu_{1/3}(IP) \geq n/2 - O(1)$.

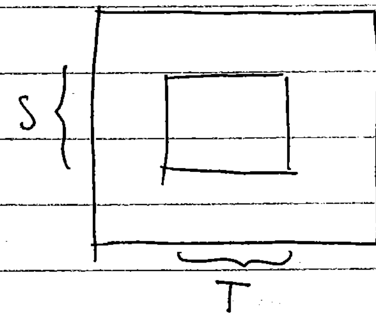
We take $\mu \sim$ uniform.

<u>Goal:</u> Prove $\mathcal{D}isc_\mu(IP) \leq \frac{1}{\sqrt{2^n}}$.

NB. This implies the bound.

Let $R = S \times T$, $S, T \subseteq \{0,1\}^n$ be any rectangle.

$$\mathrm{Disc}_\mu(R, \mathrm{IP}) = \sum_{\substack{x \in S \\ y \in T}} (-1)^{\langle x, y \rangle} \cdot \frac{1}{2^{2n}}$$



<u>Def:</u> $H_n \triangleq 2^n \times 2^n$ Hadamard matrix (orthogonal)

$$\mathrm{Disc}_\mu(R, \mathrm{IP}) = \frac{1}{2^{2n}} \cdot 1_S^t H_n 1_T, \quad \left(1_S \in \{0,1\}^{2^n} \right)$$

$$= \frac{1}{2^{2n}} \left\langle 1_S^T, H_n 1_T \right\rangle$$

$$\leq \frac{1}{2^{2n}} \underbrace{\|1_S\|_2}_{\sqrt{|S|}} \underbrace{\|H_n \cdot 1_T\|_2}_{\sqrt{2^n} \cdot \sqrt{|T|}}$$

$$\leq \frac{2^{\frac{3}{2}n}}{2^{2n}} = \frac{1}{\sqrt{2^n}}.$$

$\square$

<u>Indexing Problem:</u>

$$\text{Alice} \xleftarrow{\quad i \quad} \text{Bob}$$

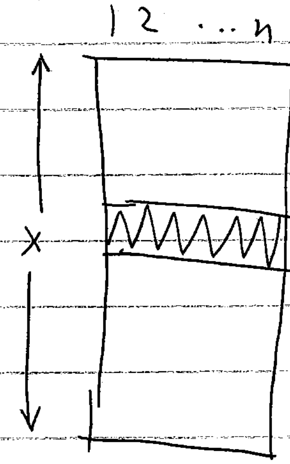
$$x \in \{0,1\}^n \xrightarrow{\quad x_i \quad} i \in \{1, \dots, n\}$$

Goal: Bob should learn x_i.

Trivial $\lceil \log n \rceil$-bit protocol.

Now, Suppose we only allow Alice to send a single message so that Bob can figure out x_i. (one-way communication).

Now the trivial solution costs n bits.
Can we do better?



Deterministic: If Alice sends $< n$ bits, Bob learns about a rectangle with ≥ 2 rows, a, b, $(a \neq b)$.

The protocol has identical behavior for (a, j), (b, j), where $a_j \neq b_j$.

$\square$

* Now, dist. complexity. (say $\mu \sim$ uniform)

Exer. Come up with a μ on $\{0,1\}^n \times [n]$ s.t. $\mathcal{D}^{\mu}_{\frac{1}{3}}(\text{Index}) = \Omega(n)$.

(Hint: take uniform dist. supported on a code of distance $\geq n/3$)

(6)

Information theoretic proof:

Alice $\xrightarrow{\quad M \quad}$ **Bob**

X uniform on $\{0,1\}^n$

M depends on the randomness in X.

i uniform on $[n]$

We **Want:** If Π is correct w.p. $2/3$ $\Rightarrow$ need long M.

Note: $CC(\Pi) \geq \log_2 \left(\text{Supp}(M) \right)$

$$\geq H(M).$$

$\Rightarrow$ Suffices to lower bound $H(M)$.

$\Rightarrow$ " " show M tells a lot about X.

$$\Rightarrow \quad CC(\Pi) \geq I(M; X).$$

(In fact, here $H(M) = I(M; X)$). since $M = M(X)$.

$$* \quad I(M; X) \geq \sum_{i=1}^{n} I(M; X_i)$$

$$= \sum_{i=1}^{n} \underbrace{H(X_i)}_{1} - H(X_i \mid M_i)$$

$$= n - \sum_{i=1}^{n} H(X_i \mid M)$$

7

But since Bob can predict X_i from M,

We can use Fano's inequality

<u>Def:</u> $p_e^{m,i}$ = Prob(Bob is wrong on X_i given that <u>$M=m$</u> is sent)

We know: $\mathbb{E}_{m\sim M, i}\left(p_e^{m,i}\right) \leq 1/3$.

* By Fano's inequality, $h\left(p_e^{m,i}\right) \geq H(X_i \mid M=m)$

$$\Rightarrow \mathbb{E}_{m\sim M}\left[h\left(p_e^{m,i}\right)\right] \geq H(X_i \mid M).$$

~~By convexity~~,

$$\mathbb{E}_{i, m\sim M}\left(h\left(p_e^{m,i}\right)\right] \geq \mathbb{E}_i\left(H\left(X_i \mid M\right)\right) = \frac{\sum_{i=1}^{n} H(X_i \mid M)}{n}$$

But by concavity of $h(\cdot)$, LHS $\leq h\left(\mathbb{E}_{i,m}\left(p_e^{m,i}\right)\right)$

$$\leq h(1/3).$$

Back to proof

$$\Rightarrow \quad CC(\Pi) \geq n - h(1/3)\cdot n = \Omega(n).$$

$\square$