Randomized (many-round) Communication complexity.

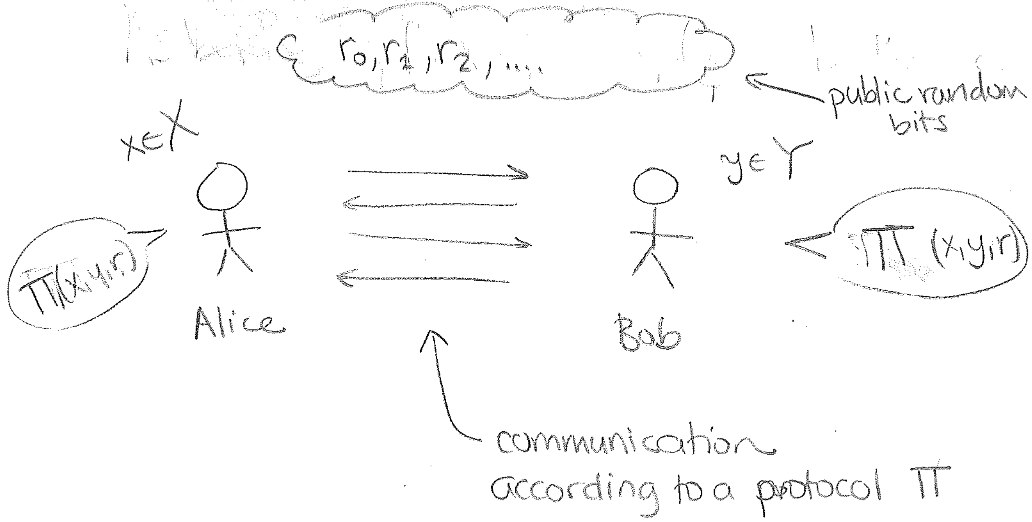
AGENDA
- Randomized CC
- Discrepancy: $R(IP) = \Omega(n)$
- Corruption: $R(DISJ) = \Omega(n)$ (sketch)

So far:

one way CC: deterministic $\vec{D}(f)$, randomized $\vec{R}(f)$

many-round CC: deterministic $D(f)$, ______ ← obviously today we are going to do randomized.

As before, let $f: X \times Y \to \{0,1\}$.



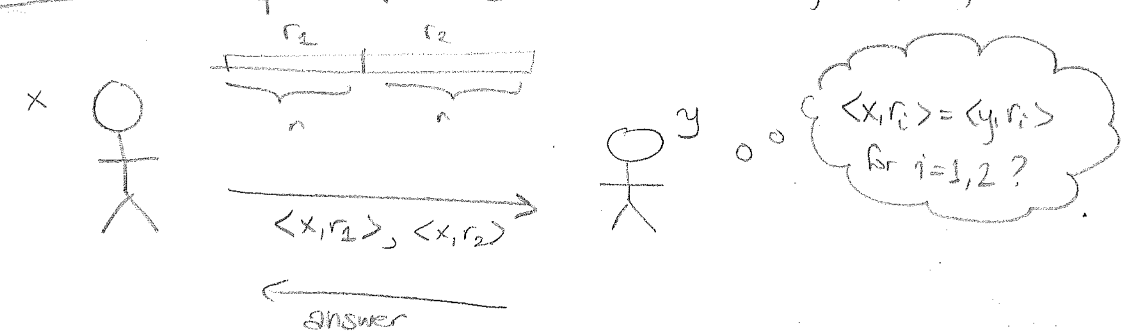
$$R_\varepsilon(f) = R_\varepsilon^{(public)}(f) =$$ smallest communication cost (in the worst case) of any protocol Π which has, $\forall x, y$.

$$\mathbb{P}_r\{\ \Pi(x,y,r) = f(x,y)\ \} \geq 1 - \varepsilon.$$

(randomization helps!)

EXAMPLE $R_{1/4}(EQ_n) = 3$ ← but $\vec{D}(EQ) = D(EQ) = \Omega(n)$

$x, y \in \{0,1\}^n$, $EQ(x,y) = \mathbb{1}_{x=y}$



(this is even one-way!)

2

Puzzle: how would you do it w/ private coins?

$$R^{private}_{1/4}(EQ) = \Theta(\log(n))$$

On HW, you'll show that an additive log(n) is the worst difference between public + private coins.

For now let's stick w/ public coins.

Lower bounds for $R_\varepsilon(f)$. ← Why? As before, this gives lower bounds for randomized algs for data structures, or randomized multi-pass streaming algs. Plus lots of other applications.

We still have Yao's Lemma, and as w/ 1-way randomized communication, we can study distributional complexity.

Def $D^\mu_\varepsilon(f)$ = communication necessary when

$x, y \sim \mu$ and the protocol succeeds w/ prob $\geq 1-\varepsilon$

dist on $X \times Y$

Yao's Lemma (for many-round CC):

$$R_\varepsilon(f) = \max_\mu D^\mu_\varepsilon(f)$$

proof of $\geq$ is similar to what we saw before

proof of $\leq$ is omitted (use von Neumann's minimax thm).

Examples.

What's left? EQ got easy w/ randomness, INDEX got easy w/ many rounds.

Today:

$R(IP_n) = \Omega(n)$ ← for this, we'll use "discrepancy" technique,

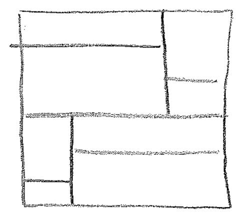
$R(DISJ_n) = \Omega(n)$ ← "corruption" technique

This one is the most useful thing if you want to prove lower bounds; tons of stuff reduces to it.

Technique 1:

DISCREPANCY

Recall the rectangle picture from last time, for a deterministic protocol Π w/ $(x,y) \sim \mu$.



- As before, Π partitions M_f into rectangles.
- Π always works $\Rightarrow$ all rectangle are monochromatic.
- Π succeeds w/ prob $1-\varepsilon$ ...

... means the rectangles are ALMOST monochromatic.

$$M_f \in \{+1,-1\}^{X \times Y}$$
$$(M_f)_{x,y} = (-1)^{f(x,y)}$$

Observation: If $D^{\mu}_{\varepsilon}(f) = t$, $\exists$ partitioning of M_f into $\leq 2^t$ combinatorial rectangles R so that

$$\sum_R \mu(R) \cdot \mathbb{P}_{\mu}\left(f(x,y) = \mathrm{MAJ}(R) \mid (x,y) \in R \right) \geq 1-\varepsilon.$$

Def The DISCREPANCY of a rectangle R is

$$\mathrm{Disc}_{\mu}(R,f) = \sum_{x,y \in R} (-1)^{f(x,y)} \mu(x,y)$$

← measure of how monochromatic R is

$$= \mathbb{P}_{\mu}(R) \cdot \left[\mathbb{P}_{\mu}\left(f(x,y)=0 \mid (x,y) \in R \right) - \mathbb{P}_{\mu}\left(f(x,y)=1 \mid (x,y) \in R \right) \right]$$

$$\mathrm{Disc}_{\mu}(f) = \max_R \mathrm{Disc}_{\mu}(R,f)$$

↖ over ALL combinatorial rects $R \subseteq X \times Y$

under uniform dist,

eg,

$$\begin{matrix} + & + & - \\ + & + & - \\ - & + & - \end{matrix}$$

- discrepancy is 0. Perfectly balanced.
- discrepancy is 1/9
- discrepancy is 4/9.

Prop $\forall f: X\times Y \to \{0,1\}$, $\forall \mu$, $\forall \varepsilon < 1/2$,

$$\left(R_\varepsilon(f) \geq \right) D^\mu_\varepsilon(f) \geq \log_2\left(\frac{1-2\varepsilon}{\mathrm{Disc}_\mu(f)}\right)$$

Pf. Any protocol Π w/ cost t, partitions into 2^t rectangles.
+ fail prob ε

$$\begin{aligned} 1-2\varepsilon &\leq \mathbb{P}(\text{success}) - \mathbb{P}(\text{failure}) \\ &\leq \mathbb{P}_\mu(\Pi(x,y) = f(x,y)) - \mathbb{P}_\mu(\Pi(x,y) \neq f(x,y)) \\ &= \sum_{l=1}^{2^t} \mathrm{Disc}_\mu(R_l, f) \\ &\leq \sum_{l=1}^{2^t} \mathrm{Disc}_\mu(f) \\ &= 2^t \cdot \mathrm{Disc}_\mu(f) \quad \blacksquare \end{aligned}$$

Example $R(IP_n) = \Omega(n)$

proof Recall M_{IP} is the Hadamard matrix
- all entries ± 1
- eigenvalues $\pm\sqrt{2^n}$, half +, half − ← indeed, $M_{IP}^2 = 2^n \cdot I$, $\mathrm{tr}(M_{IP}) = 0$

Lemma. Let f be a symmetric Boolean fn, so

$$f(x,y) = f(y,x) \in \{0,1\}$$

Then $\mathrm{disc}_{\text{uniform}}(f, A\times B) \leq 2^{-2n} \lambda_{max}(M_f) \sqrt{|A|\cdot|B|}$ (biggest in absolute value)

Pf Let v_i be eigenvectors for M_f, so $M_f v_i = \lambda_i v_i$, $\langle v_i, v_j\rangle = 0$, $\|v_i\|^2 = 1$.

$\mathbb{1}_A = \sum \alpha_i v_i$, $\mathbb{1}_B = \sum \beta_i v_i$

$$\begin{aligned} 2^{2n}\,\mathrm{disc}(f, A\times B) &= |\mathbb{1}_A^T M_f \mathbb{1}_B| \quad (\pm 1\text{-valued}) \\ &= \sum_i \alpha_i \beta_i \lambda_i \\ &\leq \lambda_{max} \sum_i |\alpha_i||\beta_i| \underset{\text{C-S}}{\leq} \lambda_{max} \|\alpha\|_2 \|\beta\|_2 \leq \lambda_{max}\sqrt{|A|\cdot|B|} \end{aligned}$$

Thus, $\operatorname{disc}_{\mu}(IP_n, A \times B) \leq 2^{-2n}\sqrt{2^n |A||B|}$, for all A, B.

μ uniform

so $\operatorname{disc}(IP_n) \leq \frac{1}{2^{2n}}\sqrt{2^n \cdot 2^{2n}} = 1/\sqrt{2^n}$, and

$R_{1/4}(IP_n) \geq \log_2\left(\frac{2^{n/2}}{2}\right) = \Omega(n)$ as desired.

By proposition.

This space intentionally blank!

Technique 2: Corruption

- We've handled IP. What about DISJ?
  - Uniform won't cut it as a hard dist anymore: Alice + Bob will just say "not disjoint" and be right whp.

Suppose we have a hard dist μ (We'll come to that in a minute).
How do we prove $D^{\mu}_{\epsilon}(f) \geq \Omega(n)$?

Idea (corruption). Suppose we had a protocol that was good on μ.

Say $A = \{(x,y) : f(x,y) = 1\}$

$B = \{(x,y) : f(x,y) = 0\}$

Let $R_1, \ldots, R_t$ be comb. rects which are almost all 1's.

Suppose we could show

(1) $\mu(A) = 3/4$

(2) $\exists \alpha, \delta, \ \forall i = 1, \ldots, t, \quad \mu(R_i \cap B) \geq \alpha \mu(R_i \cap A) - 2^{-\delta n}$

That is, (2) says that all the almost-1 rectangles that are "big enough" wrt μ (bigger than $2^{-\delta n}$) are seriously corrupted: there are a lot of 0's in them.

We can use 1 and 2 to prove a lower bound:

$$\varepsilon \geq \mu(B \cap \cup_{i=1}^{t} R_i)$$

$$= \sum_{i=1}^{t} \mu(R_i \cap B)$$

$$\geq \sum_{i=1}^{t} (\alpha \mu(R_i \cap A) - 2^{-\delta n}) \quad \text{by corruption}$$

$$\geq \alpha \cdot \underbrace{\tfrac{3}{4}(1-\varepsilon)}_{\sum_i \mu(R_i \cap A) = \mu((\Pi \text{ outputs } 1) \cap A) \geq 3/4(1-\varepsilon)} - t \cdot 2^{-\delta n}$$

Choosing ε small enough + rearranging,

$$\underset{\#\text{rectangles}}{t} = 2^{\Omega(n)}$$

So $D_\varepsilon^\mu(f) = \Omega(n)$.

Thm $\boxed{R(DISJ) = \Omega(n)}$.

[Kalyanasundaram - Schnitger '92
Razborov '92]

proof here is due to Razborov. There are also cool new ones w/ information complexity [see eg. Braverman Moitra '13]

So now the goal is to design μ so that 1 and 2 hold.
We'll just sketch it here.

Here's the distribution. Say $n = 4\ell - 1$.

- Choose a random partition $P = \{P_x, P_y, \{i\}\}$ of $[n]$, so that $|P_x| = |P_y| = 2\ell - 1$
- Draw $x \subseteq P_x \cup \{i\}$ of size ℓ uniformly at random
- Draw $y \subseteq P_y \cup \{i\}$ of size ℓ uniformly at random.

Notice, $\mathbb{P}(x \cap y \neq \phi) = \mathbb{P}(i \in x) \cdot \mathbb{P}(i \in y) = 1/4$, so 1 is satisfied. ✓

Now we just need to prove 2: Fix a rectangle $R = R_x \times R_y \subseteq 2^{[n]} \times 2^{[n]}$

The idea is to look at each partition P.
Let

$$\mathrm{Row}_0 = \mathbb{P}_{,} \{ x \in R_x \mid P,\ i \notin x \}$$
$$\mathrm{Row}_1 = \mathbb{P}_{,} \{ x \in R_x \mid P,\ i \in x \}$$

← randomness is over choice of $x \subseteq P_x$

this is fixed

$$\mathrm{Col}_0 = \mathbb{P}_{,} \{ y \in R_y \mid P,\ i \notin y \}$$
$$\mathrm{Col}_1 = \mathbb{P}_{,} \{ y \in R_y \mid P,\ i \in y \}$$

So Row_0 is the probability that a set of size l, unif at random from P_x, lives in the rows R_x

Row_1 is the same, except that we choose a set of size $l-1$, and demand that i is the l^{th} thing.

similar for Col_0, Col_1.

Intuitively, $\mathrm{Row}_0, \mathrm{Row}_1$ are pretty similar. P is GOOD if that's really the case.

Say that P is GOOD if

dependence on P suppressed

$$\mathrm{Row}_1 \geq \frac{1}{3}\mathrm{Row}_0 - 2^{-\delta n}$$

-and-

$$\mathrm{Col}_1 \geq \frac{1}{3}\mathrm{Col}_0 - 2^{-\delta n}$$

Why did we do this? We want to control

$$\mathbb{P}_{,}(B \cap R) = \frac{1}{4}\mathbb{E}_P(\mathrm{Row}_1 \cdot \mathrm{Col}_1)$$

Indeed,

recall $B = \{(x,y) : \ldots,\ x \cap y = \{i\}\}$

$$P(B \cap R) = \underbrace{P((x,y) \in R \mid i \in x,\ i \in y)}\ \cdot\ \overbrace{\mathbb{P}(B)}^{=1/4}$$

$$= \textstyle\sum_P \mathbb{P}(P) \cdot \mathbb{P}\{x \in R_x \mid P, i \in x\} \cdot \mathbb{P}\{x \in R_y \mid P, i \in y\}$$

$$= \mathbb{E}_P(\mathrm{Row}_1 \cdot \mathrm{Col}_1)$$

$$\mathbb{P}(A \cap R) = \frac{3}{4}\mathbb{E}_P(\mathrm{Row}_0 \cdot \mathrm{Col}_0) \quad \text{similarly}$$

So if P is mostly GOOD, then $\mathbb{P}(B \cap R)$ is big compared to $\mathbb{P}(A \cap R)$, which is what 2 says.

Lemma (Most partitions are good)

proofs omitted, see posted article on set disjointness for more details.

$\forall\ P_y$,

$$\mathbb{P}\{ P \text{ is bad b/c of row condition} \mid P_y \} \leq 1/5$$

$\forall\ P_x$

$$\mathbb{P}\{ P \text{ is bad b/c of col condition} \mid P_x \} \leq 1/5$$

Which is enough to imply

Lemma $\mathbb{E}_p\left(Row_0\, Col_0 \cdot \mathbb{1}_{p \text{ is bad}} \right) \leq \frac{4}{5}\, \mathbb{E}_p\left(Row_0 \cdot Col_0 \right)$

Then we're done:

$$\mu(B \cap R) = \frac{1}{4}\, \mathbb{E}_p\left(Row_1 \cdot Col_1 \right)$$

def of good

$$\geq \frac{1}{4} \cdot \mathbb{E}_p\left(\left(\tfrac{1}{3} Row_0 - 2^{-\delta n} \right)\left(\tfrac{1}{3} Col_0 - 2^{-\delta n} \right) \cdot \mathbb{1}_{p \text{ good}} \right)$$

$$\geq \frac{1}{4} \cdot \frac{1}{9}\ \mathbb{E}_p\left[Row_0\, Col_0\ \mathbb{1}_{p \text{ good}} \right] - 2^{-\delta n}$$

$$\geq \frac{1}{4}\ \frac{1}{9}\ \frac{1}{5}\ \mathbb{E}_p\left[Row_0\ Col_0 \right] - 2^{-\delta n}$$

by our lemma

$$= \underbrace{\frac{1}{4} \cdot \frac{1}{9} \cdot \frac{1}{5} \cdot \frac{4}{3}}_{\text{call this } \alpha}\ \mu(A \cap R) - 2^{-\delta n}$$

call this α and that proves 2 ∎