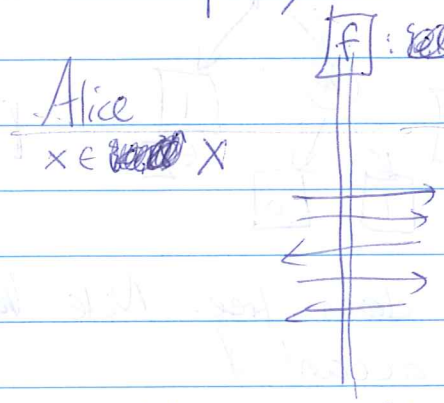
Lecture 19 - Communication Complexity

[scribe - Kushilevitz-Nisan]

[Kind of an amazing topic - beautiful "abstracting" concept w/ heavy use throughout TCS - ckt lower bounds, LP polytope bounds, ppty testing/streaming cxty, data structures...]
[We'll focus only on 2-party c.c.; multi-party is much harder]



goal: both know $f(x,y)$. [Only care about bits of comm., not comp. cost]

eg: $f = EQ_n$: • deterministic: $\leq n+1$ bits [n+1 for any fcn. This is in fact sharp...]
• Lec 9: rand.: using $O(\log n)$ bits, can succeed whp $\forall x,y$

$f = Parity_{\text{on}}$ • 2 bits

non-Boolean e.g.: $A \leftarrow$ subset of $\{1,\dots,n\}$, $B \leftarrow$ " " " " goal: median of their multiset
$O(\log^2 n)$ bits [by bin search; crucially uses interaction]

[we'll start w/ analyzing det., much easier]

[polylog = "effic." ≠ "ineff." n]

"3SAT of comm." cxty
[the most important hard problem]

$f = DISJ_n$ "disjointness"
think $x, y \subseteq [n]$
$f(x,y) = 1$ iff $x \cap y = \emptyset$
$= \neg \bigvee_{i=1}^{n} (x_i \wedge y_i) = \bigwedge_{i=1}^{n} NAND(x_i, y_i)$

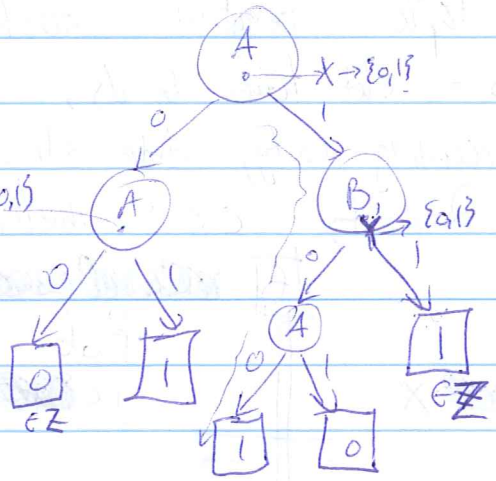
Det. complexity: $n+1$ [we'll see]
Rand. complexity: $\Omega(n)$ [KS '92]

[so go to hard fcn: $f = IP_2$, $f(x,y) = \sum_{i=1}^{n} x_i y_i \bmod 2$. / Equiv: $f(x,S) = \chi_S(x)$] hard!!!

[Definition seems a bit wishy-washy. How to formalize?]

Comm. protocol: $\mathcal{P}$:

[tree]



[nodes labeled by who speaks]

[node has a map from speaker's domain to the msg bit]

[leaves labeled by $\mathcal{Z}$ elts]

input $x \in X$
$y \in Y$

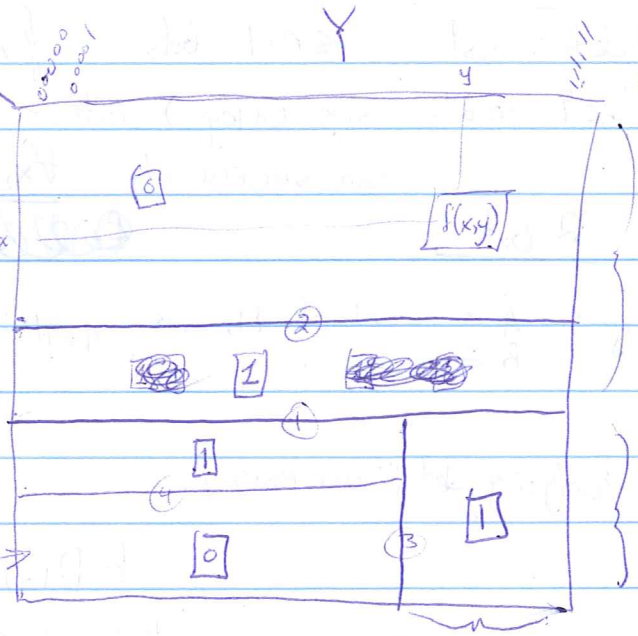
[Say in words how progress down tree. Note that the conversation can take "history" into account.]

$cost(x,y)$ = path len. on (x,y). $\quad cost(\mathcal{P}) = \max_{x,y} \{cost(x,y)\}$.

$D(f)$ = least cost of $\mathcal{P}$ comp'ing f

[Another view: rectangles]

Comm. mtx M_f:



x s.t. first bit comm'd is 0

Called "combinatorial rectangles":

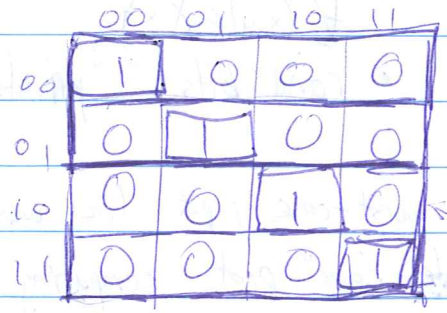
sets of form $R = K \times L$, $K \subseteq X$, $L \subseteq Y$.

[inputs in Y s.t. B says 1 @2 given A said 1 @1]

Usually K, L drawn "contiguously", but need not be.

thm: Any c-bit (det'ic, correct) comm. protocol for $f: X \times Y \to Z$ partitions M_f into $\leq 2^c$ comb. rectangles, each of which is "f-monochromatic" (i.e. f is constantly 0 or 1 on the rectangle).

e.g. EQ_2, naive prot:



→ 3 bits, 8 monoch. rects

this row has rects $\{10\} \times \{00, 01, 11\}$, $\{10\} \times \{10\}$

thm: $D(EQ_n)$ is $\geq n+1$ ($\Rightarrow = n+1$)

pf: • M_{EQ_n} has 2^n 1's on its diag.
• Each must be in a little 1×1 comb. rect.
• 0's must also be in ≥ 1 [actually, $\gg 1$] rect.

$\therefore \geq 2^n + 1$ rects, $\Rightarrow c \geq \lceil \log_2(2^n + 1) \rceil = n+1$. □

(Pf: Say $(x,x) \in K \times L$. Can't have $K \supseteq \{x\}$ or $L \supseteq \{x\}$.)

thm: [Melhorn-Schmidt '82] hmwk: $D(f) \geq \log(2 \cdot \text{rank}_{\mathbb{R}}(M_f) - 1)$

hint: [comb rects have rank 1]

cor: $D(EQ_n) \geq n+1$

cor: $D(DISJ_n) \geq n+1$ [sketch]

pf: $M_{DISJ_n} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{\otimes n}$ [ex]

$\therefore$ [ex] $\text{Rank}_{\mathbb{R}} = \left(\text{rank}_{\mathbb{R}} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right)^n = 2^n$

$\therefore D(\cdot) \geq \log(2^n - 1)$. □

[Famous] Log-Rank Conj [LS '88]: $D(f) \leq \text{polylog}(\text{rank}(M_f))$.

Best known: $D(f) \leq \tilde{O}(\sqrt{\text{rank}(M_f)})$ [Lov '13]

$\geq$ sometimes $(\log \text{rank})^{\log_3 6}$ [Kush '94]

[[Det. c.c. is slightly boring, actually, b/c too restrictive. Algs are too weak. Rand. c.c. is totally where it's at.]]

Randomized c.c.: • Players base communication also on rand bits
• Worst-case w/r/t inputs: require that $\forall (x,y) \in X \times Y$, output $f(x,y)$ w.h.p., using $\leq c$ bits
• rand. bits: "private" or "public"?

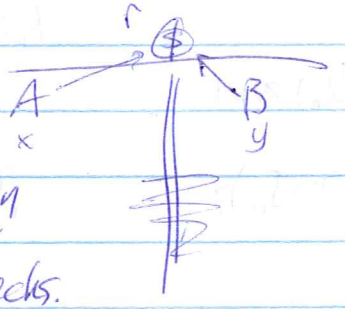
def: $R_\varepsilon^{pri}(f)$ = #bits comm. on worst-case input (incl. worst-case randomness) for a "private-coins" prot. computing $f(x,y)$ w.p. $\geq 1-\varepsilon$ on all inputs

e.g. [Lec 9]: $R_{\frac{1}{3}}^{pri}(EQ_n) \leq O(\log n)$. Pf: [[Alice interps x as coeffs of deg-n poly mod prime $\approx 3n$. Sends p & eval. of poly on rand input. Uses fact that two deg n polys agree on $\leq n$ inputs]]

Reed-Sol. special case of...
• A, B agree on an "asymp. good" $[O(n), n, \cdot]_2$ code Enc
• Alice sends $(i, Enc(x)_i)$ for $O(1)$ many rand i. Bob checks. [not impl]

[[Rem: the $O(\log n)$ expense is from sending the code positions. Given "public randomness" could avoid that. Could use a code w/ awesome dist., like Hadamard code]]

prop: $R_{\frac{1}{3}}^{pub}(EQ_n) \leq$ 2 !



pf: [Interp pub. rand. as two strs $r_1, r_2 \in \mathbb{F}_2^n$]
• A sends $r_1 \cdot x$, $r_2 \cdot x$ mod 2. Bob checks.

□

[[So is "public coins" a big cheat? Actually, no!]]

Obvious: $R_\varepsilon^{pub}(f) \leq R_\varepsilon^{pri}(f)$ [[Why? Alice/Bob can just use every other bit]]

[[this additive $+O(\log n)$ diff is worst poss]]

Newman's Theorem: Can convert public coins prot to priv. coins using with $+\delta$ addit. error using just $+O(\log n + \log 1/\delta)$ comm bits.

[[$R^{priv}_{\varepsilon+\delta}(f) \le R^{pub}_{\varepsilon}(f) + O\left(\frac{\log n + \log 1/\delta}{\log |X||Y|}\right)$]].

pf: Say public prot. uses an m-bit rand string.

Private prot:

① A,B jointly write down $t = O(n/\delta^2)$ rand strs $r^{(1)}, \dots, r^{(t)} \in \{0,1\}^m$.

② Go to sep. rooms, get inputs x, y.

③ A chooses $i \sim [t]$ uniformly, tells Bob: $O(\log n + \log 1/\delta)$ bits

④ They do public prot using r_i.

Chernoff bound: for fixed (x,y) [prob they're a bad sample] $\le 2^{-2n}$

$\therefore$ union bound: $\forall (x,y)$ this gives correct answer w.p. $\ge 1-\varepsilon-\delta$.

④ can be elim'd by Prob. Method: $\exists$ fixed choice of $r^{(1)}, \dots, r^{(t)}$ which works.

Sketch:

Chernoff: For fixed $(x,y) \in \{0,1\}^n \times \{0,1\}^n$,

$$\Pr_{r^{(1)}, \dots, r^{(t)}}\left[\operatorname{avg}_{i \in [t]} \{ \mathbb{1}_{\text{error using } i} \} > \varepsilon + \delta \right] \le \exp(-\delta^2 \cdot t) < 2^{-2n}.$$

$\therefore$ by union bound over (x,y), $\exists$ fixed $r^{(1)}, \dots, r^{(t)}$ for step ④ s.t. error $< \varepsilon + \delta$ $\forall (x,y)$. □

rem:

- Public coins model is nicer — it's "the standard". $R_\varepsilon(f) := R^{pub}_\varepsilon(f)$.
- Also viewable as a prob. distrib. over cost-c det. prots.

Cost-c public coins prot $\Rightarrow$ [[A & B use the public rand bits to agree on a det prot.]].

$$\text{err.} = \max_{(x,y)} \{ \text{frac. of det prots wrong on } (x,y) \}$$

STET

[KS]: $R_{\frac{1}{3}}(DISJ_n) \geq \Omega(n)$. [How to prove? Quite hard. First step always same, tho.]

[Forget A&B. Imagine a 2-player game.]

P1: Announces $(x,y) \in X \times Y$
P2: Announces cost-c det prot. } simul.

Payoff: +1 to P1 if prot. errs on (x,y).

[One more notion of rand. c.c.] Let μ be a prob. dist on inputs (x,y)

def: $D^{\mu}_{\varepsilon}(f)$ = least cost of det. prot. P s.t. $\Pr_{(x,y)\sim\mu}[P(x,y)=f(x,y)] \geq 1-\varepsilon$

Distrib. comm. cxty

rand? ← it's equiv. If $\Pr_{(x,y)\sim\mu}\left[\Pr_{r}[P_r(x,y)=f(x,y)]\right] \geq 1-\varepsilon$

$\exists r_0$ s.t. P_{r_0} is det.

cor: $\forall \mu$, $R'_{\varepsilon}(f) \geq D^{\mu}_{\varepsilon}(f)$

pf: [prot achieving this has err $\leq \varepsilon$ on all inputs, hence on any avg. of inputs]

rem: (exercise) $R_{\varepsilon}(f) = \max_{\mu}\{D^{\mu}_{\varepsilon}(f)\}$. [I.e., there's a "worst" input dist.]

pf: Minimax...

Cor: To show $R_{\varepsilon}(DIST_n) \geq c$, sufficient (and nec.) to find a "hard distrib." μ on $X \times Y$, show any det. prot. communicating $< c$ bits errs on $> \varepsilon$ frac. of inputs under μ.

"Yao's (Minimax) Principle" (somewhat easier)

---

thm: $D^{\mu}_{\frac{1}{4}}(IP_2) \geq \frac{n}{2} - 1$ when μ is unif. distrib.

rec: $IP_2(x,S) = \chi_S(x) \in \{-1,1\}$.

$\{-1,1\}^n \to [n]$

Pf: Let Π be a det. prot. using $\le c$ bits.

Think $\Pi: (x,S) \mapsto \{-1,1\}$, partitions inputs into $\le 2^c$ rects

$$R_1 \times \mathcal{S}_1, \dots, R_{2^c} \times \mathcal{S}_{2^c}$$

(R_i: collection of strings x; $\mathcal{S}_i$: collection of subsets S.)

Labels each with some $z_1, \dots, z_{2^c} \in \{-1,1\}$.

Goal: Π, IP_2 agree on $\ge \frac{3}{4}$ of inputs (x,S) (drawn unif)

$\Rightarrow c \ge \frac{n}{2} - 1$

Suppose so: $\mathop{E}_{\substack{x \sim \{-1,1\}^n \\ S \sim [n]}} [\Pi(x,S) \cdot IP_2(x,S)] \ge \frac{1}{2}$.

$$= \mathop{E}_{x,S}\left[\sum_{i=1}^{2^c} \mathbb{1}_{R_i}(x)\,\mathbb{1}_{\mathcal{S}_i}(S)\, z_i\, IP_2(x,S)\right]$$

$$\le \sum_{i=1}^{2^c} \left|\mathop{E}_{x,S}\left[\mathbb{1}_{R_i}(x)\,\mathbb{1}_{\mathcal{S}_i}(S)\, IP_2(x,S)\right]\right|$$

← "discrepancy of IP_2 on rect. $R_i \times \mathcal{S}_i$ under unif."

Claim: $\le 2^{-n/2}$ $\forall R_i, \mathcal{S}_i$.

$\Rightarrow 2^c \cdot 2^{-n/2} \ge \frac{1}{2} \Rightarrow c \ge n/2 - 1$.

$$= \left|\mathop{E}_{x,S}\left[\mathbb{1}_{R_i}(x)\,\mathbb{1}_{\mathcal{S}_i}(S) \cdot \chi_S(x)\right]\right|$$

$$= \left|\mathop{E}_{S}\left[\mathbb{1}_{\mathcal{S}_i}(S) \cdot \mathop{E}_{x}\left[\mathbb{1}_{R_i}(x)\chi_S(x)\right]\right]\right| \qquad \widehat{\mathbb{1}_{R_i}}(S)$$

$$= \left|\mathop{E}_{S}\left[\mathbb{1}_{\mathcal{S}_i}(S) \cdot \widehat{\mathbb{1}_{R_i}}(S)\right]\right|$$

$$\le \sqrt{\mathop{E}_{S}\left[\mathbb{1}_{\mathcal{S}_i}(S)^2\, \widehat{\mathbb{1}_{R_i}}(S)^2\right]}$$

$$\le \sqrt{2^{-n} \sum_S \widehat{\mathbb{1}_{R_i}}(S)^2} = 2^{-n/2}\sqrt{\mathop{E}_x[\mathbb{1}_R(x)^2]} \le 2^{-n/2}$$

(Pars.) □

ex: $D^{\text{unif}}_{1/4}(D|S|_n) \le O(1)$.

thm: $D^{\text{prod dist}}_{1/4}(D|S|_n) \le \tilde{O}(\sqrt{n})$.

To prove $R_{1/4}(D|S|_n)$ $\ge \Omega(n)$ need non-prod dist. Hard.

Best proof uses info thy....