1

Thu 4/4

Lemma: $R_{1/3}(f) \geq \Omega(\log D(f))$.

$$D(f) \leq 2^{O(R(f))}.$$

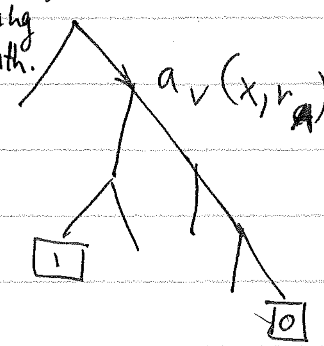
Proof idea: Estimate $\Pr(\Pi(x,y)=0)$ within $\frac{1}{10}$.

For each leaf ℓ, labeled 0,

* Alice sends p_ℓ^A = Prob, given x, of her randomness following edges on the root to ℓ path.

Bob computes p_ℓ^B: prob., given y, of his randomness following root-to-ℓ path.

Estimate $\sum_{\ell,\ \text{label}=0} p_\ell^A p_\ell^B$



---

* **Public coin protocols.**

$\boxed{\text{Shared public randomness}}$ (of arbitrary length)

(some dist. D)

Alice   Bob

x $\longrightarrow$ y

$\longleftarrow$

$\longrightarrow$

$\vdots$

Equivalently, a public coin randomized protocol is a distribution over deterministic ones.

Fix r, get a deterministic protocol $\pi^{(r)}$.

$$\Pr\left(\pi(x,y) = f(x,y)\right] = \Pr_{r\leftarrow D}\left[\pi^{(r)}(x,y) = f(x,y)\right]$$

for computing f

$(\text{error}_{\pi}(f))$ Error of π $= \max_{x,y}\left[\Pr\left(\pi(x,y) \neq f(x,y)\right)\right]$

Def. $$R_{\varepsilon}^{pub}(f) = \min_{\substack{\pi \\ \text{error}_{\pi}(f)\le\varepsilon}} \left[CC(\pi)\right]$$

Lemma (easy): $R_{\varepsilon}^{pub}(f) \le R_{\varepsilon}(f)$

proof: Obvious!

$\square$

$R_{1/3}^{pub}(EQ) = ?$ $\left(\text{know: } \le O(\log n)\right)$

$\boxed{h}$ → (The hash family can now be larger!)

Alice $\xrightarrow{h(x)}$ Bob

$h(x) \stackrel{?}{=} h(y)$

Can we do better than $O(\log n)$?

Yes, by using a very large hash family that hashes to a const # of bits.

(3)

Protocol:

$$r \in \{0,1\}^n$$

$$\text{Alice } (x) \xrightarrow{\; b = \langle x, r\rangle \bmod 2 \;} \text{Bob}$$

$$\xleftarrow{\;\text{result.}\;} \quad \text{Check if } \langle y, r\rangle = b$$

(2 bits of communication!)

If $x \neq y \Rightarrow x - y \neq 0 \Rightarrow \Pr_r(\langle x-y, r\rangle = 0) = \frac{1}{2}$.

(repeat to get error $\leq \frac{1}{3}$).

$\square$

$$\Rightarrow R^{pub}_{1/3}(EQ) = O(1).$$

Lemma: (Newman's Lemma)

$$\forall \varepsilon, \delta > 0, \; R_{\varepsilon+\delta}(f) \leq R^{pub}_{\varepsilon}(f) + O\left(\log \frac{n}{\delta}\right).$$

($\Rightarrow$ public coin can only save an additive log and typically it's as good just to work with public coin).

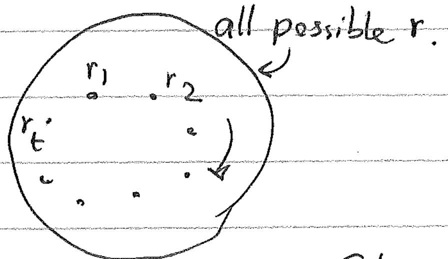
Proof: (1) (Reduce randomness)

Convert to public coin that only uses $O(\log \frac{n}{\delta})$ random bits and error $\varepsilon + \delta$.

(2) Alice generates the randomness and sends to Bob.

$\square$

<u>How to do (1)?</u>



$$\forall x, y, \quad \Pr_{r \leftarrow D}\left[\Pi^{(r)}(x,y) \neq f(x,y)\right] \leq \varepsilon.$$

<u>Claim.</u> $\exists\, r_1, \ldots, r_t, \quad t \leq \mathrm{poly}\left(\frac{n}{\delta}\right)$

such that $\displaystyle \Pr_{\substack{i \leftarrow \{1,\ldots,t\} \\ \text{uniformly}}}\left[\Pi^{(r_i)}(x,y) \neq f(x,y)\right] \leq \varepsilon + \delta$

<u>Pf (of Claim):</u> By standard Chernoff-Hoeffding bounds. (using the probabilistic method)

Fix (x,y). Pick $r_1, \ldots, r_t$ u.a.r according to D.

<u>Bad event:</u> $\#\, i$ for which $\Pi^{(r_i)}(x,y) \neq f(x,y) > (\varepsilon+\delta)t$.

$\Pr(\text{bad event}) \leq 2^{-\Omega(\delta^2 t)}$.

Union bound over $(x,y) \rightarrow \Pr(\text{bad}) \leq 2^{2n - \Omega(\delta^2 t)}$.

$$\Rightarrow \Pr\left(\exists (x,y) \text{ s.t. } \#\{i \mid \pi^{(r_i)}(x,y) \neq f(x,y)\} \geq (\varepsilon+\delta)t\right) < 1$$

by the choice of t.

$\square$

<u>Exercise:</u> $R^{pub}_{1/3}(GT) \leq O(\log^2 n)$.

$(GT(x,y) = 1 \text{ iff } x > y)$

improve to $R^{pub}_{1/3}(GT) \leq O(\log n \cdot \log\log n)$

(in fact $O(\log n)$ is possible.)

<u>Def.</u> (Distributional Complexity)

Protocol : Deterministic.

But inputs : Random.

For det. protocol π, dist μ on (x,y),

$$\text{error}^{\mu}(\pi, f) \triangleq \Pr_{(x,y)\leftarrow\mu}\left(\pi(x,y) \neq f(x,y)\right)$$

(depends on μ, of course)

6

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

Dist μ on $X \times Y$, $\varepsilon \in (0, \frac{1}{2})$.

$$\mathcal{D}^{\mu}_{\varepsilon}(f) \triangleq \min_{\substack{\Pi,\ \text{det.} \\ err^{\mu}(\Pi, f) \leq \varepsilon}} \left[CC(\Pi) \right].$$

Example: $\mathcal{D}^{\text{uniform}}_{1/3}(EQ) = 0$

(do nothing!)

now, DISJ : $\mathcal{D}^{\text{uniform}}_{1/10}(\text{DISJ}) = 0$, since

$$\Pr_{(x,y) \sim \text{uniform}}\left(\text{DISJ}(x,y) = 1 \right) = \left(\frac{3}{4}\right)^n.$$

(protocol just says "NO")

Birthday paradox suggests that

(x, y) should have size $\sim \sqrt{n}$ for

DISJ to be interesting

$\Rightarrow \mu_{\sqrt{n}} \triangleq$ Set $\left| \begin{array}{l} X_i = 1 \quad \text{w.p. } \frac{1}{\sqrt{n}} \\ (Y_i = 1) \ (\text{independently}) \end{array} \right.$, iid.

Side remark: (Same happens if x (y) is chosen uniformly at random among sets of size $\sqrt{n}$.)

Challenge: What is $D^{\mu_{\sqrt{n}}}_{\frac{1}{100}}(DISJ) = ?$

Obvious upper bound: $O(\sqrt{n} \cdot \log n)$
(just send the set bits)
Can we do better? (Exercise)

Lemma: $\forall \mu,\ R^{pub}_{\varepsilon}(f) \geq D^{\mu}_{\varepsilon}(f)$.

i.e., to prove lower bounds on R^{pub}_{ε}, come up with some μ over which det. protocols ~~are~~ have large CC.

Given public coin protocol $\pi^{(r)}$,

$$\forall (x,y), \quad \Pr_r\left[\pi^{(r)}(x,y) \neq f(x,y)\right] \leq \varepsilon.$$

$$\Rightarrow \Pr_{r,(x,y)\sim\mu}\left[\pi^{(r)}(x,y) \neq f(x,y)\right] \leq \varepsilon$$

$$\Rightarrow \exists r \text{ s.t. } \Pr_{(x,y)\sim\mu}\left[\quad " \quad\right] \leq \varepsilon.$$

$\square$

* In fact, $R^{pub}_{\varepsilon}(f) = \max_{\mu} D^{\mu}_{\varepsilon}(f)$.
(Proof by Yao's minimax)