Thu 4/4

Lemma: \( R_{H_3}(f) \geq \omega(\log D(f)) \).
\( D(f) \leq 2^\Theta(R(f)) \).

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

For each leaf \( l \), labeled 0,

Alice sends \( p_A = \text{Prob, of her randomness} \)

Bob computes \( p_B = \text{prob., given } y \), of his randomness following root-to-1 path.

Estimate \( \sum p_A p_B \) for each \( l \), label = 0.

*Public coin protocols:*

Shared public randomness (of arbitrary length)

Alice \( X \)

Bob \( Y \)

\( \vdots \)

Equivalently, a public coin randomized protocol is a distribution over deterministic ones.
Fix $r$, get a deterministic protocol $\Pi^r(r)$.

\[ \Pr \left( \Pi(x, y) = f(x, y) \right) = \Pr_{\Pi} \left[ \Pi^r(x, y) = f(x, y) \right] \]

for computing $f$.

(error $f$) Error of $\Pi^r = \max_{x, y} \left[ \Pr_{\Pi} \left( \Pi(x, y) \neq f(x, y) \right) \right]$

**Def.** $R^\text{pub}_\varepsilon(f) = \min_{\Pi \text{ error } \leq \varepsilon} \left[ \text{CC}(\Pi) \right]$

**Lemma (easy):** $R^\text{pub}_\varepsilon(f) \leq R^\varepsilon_\varepsilon(f)$

**proof:** Obvious!

\[ R^\text{pub}_{1/3}(\text{EQ}) = \quad \left( \leq O(\log n) \right) \]

(The hash family can now be larger!)

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

Yes, by using a very large hash family that hashes to a constant # of bits.
Protocol: \( r \in \{0, 1\}^n \)

Alice: \( b = \langle x, r \rangle \mod 2 \rightarrow Bob \)

\[ x \quad \text{result. Check if} \quad \langle y, r \rangle = b \]

(2 bits of communication)

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

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

\[ \Rightarrow R^{\text{pub}}_{\frac{1}{3}} (\text{EQ}) = O(1). \]

Lemma: (Newman's Lemma)

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

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

Proof: 1. \( \text{Guessment (Reduce randomness)} \)

Convert to public coin that only uses \( O\left(\log \frac{n}{\delta}\right) \) random bits and error \( \varepsilon + \delta \).
(2) Alice generates the randomness and sends to Bob.

How to do ①?

∀x, y, all possible r.

Pr \left[ \prod_{i \in D} (x_i, y) \neq f(x, y) \right] \leq \varepsilon.

Claim: \exists \, r_1, \ldots, r_t, \quad t \leq \text{poly} \left( \frac{n}{\delta} \right)

such that \forall i \neq \{1, \ldots, t\} \text{ uniformly}

\text{Pr (of Claim): By standard Chernoff-Hoeffding bounds. (using the probabilistic method)}

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

Bad event: \# \text{ for which } \prod_{i \in D} (x_i, y) \neq f(x, y) > (3 + \delta) t.

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

Union bound over \( (x, y) \rightarrow \text{Pr (bad)} \leq 2^{2n - \Omega(\delta^2 t)}. \)
\[ \Pr(\exists (x, y) \text{ s.t. } \# \{ i \mid \prod^{(r)}(x, y) \neq f(x, y) \geq (3+\Delta)\} < 1) \]

by the choice of \( t \).

Exercise: \( R_{1/3}^{\text{pub}}(\text{GT}) \leq O(\log^2 n) \).

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

improve to \( R_{1/3}^{\text{pub}}(\text{GT}) \leq O(\log n \cdot \log \log n) \)

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

Def. (Distributional Complexity)

Protocol: Deterministic.

But inputs: Random.

For det. protocol \( \Pi \), dist \( \mu \) on \((x, y)\),

\[ \text{error}^{\mu}(\Pi, f) \triangleq \Pr_{(x, y) \sim \mu} \left( \prod^{(r)}(x, y) \neq f(x, y) \right) \]

(dependent on \( \mu \), of course)
Def.: \( f: X \times Y \to \{0, 1\} \).

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

\( D^\mu \varepsilon (f) \triangleq \min \left[ \text{CC}(\pi) \right] \).

\[ \text{Err}^\mu (\pi, f) \leq \varepsilon \]

Example: \( D^{\text{uniform}}_{\frac{1}{2}} (\text{EQ}) = 0 \) (do nothing!)

Now, \( \text{DISJ}: D^{\text{uniform}}_{\frac{1}{10}} (\text{DISJ}) = 0 \), since

\[ \Pr (\text{DISJ}(x,y) = 1) = \left(\frac{3}{4}\right)^n. \]

\((x,y) \sim \text{uniform}\) (protocol just says "No".)

\( \text{Birthday paradox suggests that}\)

\( (x,y) \) should have size \( \sim \sqrt{n} \) for \( \text{DISJ} \) to be interesting

\[ \Rightarrow \mu \overset{\Delta}{=} \text{Set } \left| X_i = 1 \text{ w.p. } \frac{1}{\sqrt{n}}, \ i.i.d. \right| \]

\[ (y_i = 1) \text{ (independently)} \]
Remark: (Some happens if $x \cdot y$ is chosen uniformly at random among sets of size $\sqrt{n}$.)

**Challenge:** What is $D^\frac{\sqrt{n}}{100} (\text{DISJ}) =$?

Obvious upper bound: $O(\sqrt{n} \cdot \log n)$

(just send the set bits)

Can we do better? (Exercise)

**Lemma:** $\forall \mu, \mathbb{E}^\text{pub}_\mu (f) \geq D_\epsilon^\mu (f)$.

i.e., to prove lower bounds on $\mathbb{E}^\text{pub}_\mu$, come up with some $\mu$ over which det. protocols have large $\epsilon$.

Given public coin protocol $\Pi^{(r)}$, \forall $(x, y)$, $\mathbb{P}_r \left[ \Pi^{(r)} (x, y) \neq f(x, y) \right] \leq \epsilon$.

$\Rightarrow \mathbb{P}_r \left[ \Pi^{(r)} (x, y) \neq f(x, y) \right] \leq \epsilon$

$\Rightarrow \exists r \text{ s.t. } \mathbb{P}_{(x, y) \sim \mu} \left[ \Pi^{(r)} (x, y) \neq f(x, y) \right] \leq \epsilon$.

$\ast$ In fact, $\mathbb{E}^\text{pub}_\mu (f) = \max_\mu D_\epsilon^\mu (f)$.