Last time:

- finish missing piece from 2^{-d} corr. bd:
  $Cor[F, P] \le U_{d+1}(F)^{2^{-(d+1)}}$ for $P = e(p)$, p deg d
- Basic Tools for PRGs:
  - k-wise indep. RV's → s.l. $k \cdot \log n$
  - ε-biased RV's → s.l. $O(\log \frac{n}{\varepsilon})$
  - k-wise indep ε-biased RV's
    ↳ s.l. $O(k + \log\frac{1}{\varepsilon} + \log\log n)$.

Today:
- basic Fourier analysis over $\{0,1\}^n$, simple applica. of
  - fooling size-s DTs
  - fooling k-juntas better
- sandwiching approximators & fooling
- Ⓐ Viola's thm: sum of d ε-biased RVs fools DEG_d.

Scribe: Mark (thanks!)

Questions?

(Prelim. project proposal due Thurs)

Fourier interlude

AOBF analysis of Boolean fns (O'Donnell)

Basics: $f: \{0,1\}^n \to \mathbb{R}$.

All ↗ form a 2^n-dim. vector space,

with inner product given by (one dim. for each x)

$$\langle f, g \rangle = \mathop{\mathbb{E}}_{x \sim \mathcal{U}_n} [f(x) \cdot g(x)]$$

so $\|f\| = \sqrt{\langle f, f \rangle}$.

Basis?

Claim: The set $(\chi_S)_{S \subseteq [n]}$ (all 2^n char fns; $\chi_S(x) = (-1)^{\sum_{i \in S} x_i}$) is an orthonormal basis for our vector space.

Pf: Need to show
- $\langle \chi_S, \chi_S \rangle = 1 \quad \forall S$ ✓
- $\langle \chi_S, \chi_T \rangle = 0$ if $S \neq T$.

$$\langle \chi_S, \chi_T \rangle = \mathop{\mathbb{E}}_{x \sim \mathcal{U}_n} [\chi_S(x) \chi_T(x)] = \mathbb{E}\left[(-1)^{\sum_{i \in S} x_i + \sum_{j \in T} x_j}\right]$$

$$= \mathbb{E}\left[(-1)^{\sum_{j \in S \Delta T} x_j}\right] = \mathbb{E}[\chi_{S \Delta T}(x)]$$

$S = T$: $S \Delta T = \emptyset$, $(-1)^0 = 1$

$S \neq T$: showed last time $\mathbb{E}[\chi_{S \Delta T}(x) = 0]$.

∎

So any $f: \{0,1\}^n \to \mathbb{R}$ has a unique rep. as lin comb. of basis elts.

Write $\hat{f}(S)$ as coeff of χ_S in:

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \cdot x_S(x).$$

$\hat{f}(S)$: Fourier coeff's of f. ?

$$\langle f, x_S \rangle = \mathop{\mathbb{E}}_{U}[x_S(U) \cdot f(U)]$$

$$= \mathbb{E}\Big[x_S(U) \cdot \sum_{T \subseteq [n]} \hat{f}(T) x_T(U)\Big]$$

$$= \sum_{T} \hat{f}(T) \cdot \underbrace{\mathbb{E}[x_S(U) x_T(U)]}_{= 1 \text{ if } S=T,\ 0 \text{ o/w}}$$

$$= \hat{f}(S).$$

So $\hat{f}(S)$ measures correl. of f & x_S.

Note $\hat{f}(\emptyset) = \mathbb{E}[f(x) \cdot \overbrace{x_\emptyset(x)}^{\equiv 1}] = \mathbb{E}[f]$.

Sometimes nice to view $f: \{-1,1\}^n \to \mathbb{R}$.

Then $$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \cdot \prod_{i \in S} x_i$$

& Fourier rep $\equiv$ rep. as multilin. poly.

Plancherel's identity: For any $f, g: \{0,1\}^n \to \mathbb{R}$,

have

$$\langle f, g \rangle = \mathbb{E}[f(U) \cdot g(U)]$$

$$= \mathbb{E}\left[\left(\sum_S \hat{f}(S) x_S\right) \cdot \left(\sum_T \hat{g}(T) x_T\right)\right]$$

$$= \sum_{S,T} \hat{f}(S) \cdot \hat{g}(T) \cdot \mathop{\mathbb{E}}_U [x_S(U) x_T(U)]$$

(1 iff $S = T$, 0 o/w)

$$= \sum_S \hat{f}(S) \cdot \hat{g}(S)$$

Special case: $f = g$. Gives (Parseval)

$$\|f\|^2 = \mathop{\mathbb{E}}_U[f(U)^2] = \sum_S \hat{f}(S)^2.$$

If $f: \{0,1\}^n \to \{-1,1\}$, then

$$\|f\|^2 = \mathbb{E}[f^2] = 1 = \sum_{S \subseteq [n]} \hat{f}(S)^2$$

OHP: Write Fourier rep. of

$$IP: \{0,1\}^n \to \{\pm 1\}, \quad IP(x_1, \ldots, x_n) = (-1)^{x_1 x_2 + x_3 x_4 + \ldots x_{n-1} x_n}.$$

Infer that $\forall$ deg-1 $\mathbb{F}_2$ poly $p(x)$, have

$$\Pr_U[IP(U) = p(U)] = \frac{1}{2} \pm \frac{1}{2^{n/2}}.$$

Def (Fourier L_1 norm) $\quad f: \{0,1\}^n \to \mathbb{R}$,

$$L_1(f) = \sum_{S \subseteq [n]} |\hat{f}(S)|.$$

Fact: If $f: \{0,1\}^n \to [-1,1]$, have $L_1(f) \leq 2^{n/2}$.

Pf: $L_1(f) = \sum_{S \subseteq [n]} |\hat{f}(S)|$

$$\overset{C\text{-}S}{\leq} \sqrt{2^n \cdot \sum_{S \subseteq [n]} \hat{f}(S)^2}$$

$$= \sqrt{2^n \cdot \mathbb{E}[f(U)^2]} \leq \sqrt{2^n} \quad \text{b/c } |f(x)| \leq 1 \text{ always.}$$ ∎

Applic. to PRGs

Recall "Dineε" for PRGs.

Lemma (Dineε): Let $f_1, \ldots, f_t : \{0,1\}^n \to \mathbb{R}$,
let $\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{R}$,
let $f(x) = \lambda_0 + \sum_{i=1}^{t} \lambda_i f_i(x)$.

If X ε_i-fools each f_i $\quad i \in [t]$, then
X ε-fools f, where $\varepsilon = \sum_{i=1}^{t} |\lambda_i| \cdot \varepsilon_i$.

This + ε-biased RV def ⇒

Cor: If X is δ-biased RV over $\{0,1\}^n$, then X fools $f: \{0,1\}^n \to \mathbb{R}$ with error $\delta \cdot L_1(f)$.

OHP: Let $f: \{0,1\}^n \to \{0,1\}$ be conj. of literals over distinct vars, eg.

$$x_1 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_6$$

Show $L_1(f) = 1$.

Last time: 0-fooled depth-d DTs using d-wise indep. (s.l. $d \cdot \log n$).

Now: fool size-s DTs.

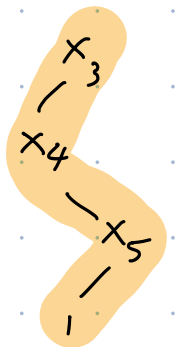
Claim: If X is δ-biased RV over $\{0,1\}^n$, then X fools size-s DTs with error δs.

(So get ε-PRG for DT_s with s.l. $O(\log s + \log n + \log \frac{1}{\varepsilon})$.)

Pf: Let T = size-s DT.

L = set of 1-leaves

f_ℓ = conj. corr. to 1-leaf ℓ.



Have $f(x) = \sum_{\ell \in L} f_\ell$.

So $L_1(f) \le \sum_{\ell \in L} L_1(f_\ell) \le |L| \le s$. Done, by prev. cor. ∎

Note: easy, given size-s DT T, to

exactly compute $\Pr_u[T(u)=1]$:

it's $\sum_{\substack{1\text{-leaf} \\ \ell}} 2^{-\text{depth}(\ell)}$.

Let's fool k-juntas better, (last time: s.t. $k \cdot \log n$)

using k-wise ε-biased:

Claim: If X is k-wise ε-bias RV over $\{0,1\}^n$, then X fools $\{-1,1\}$ valued k-juntas with error $\underbrace{\delta \cdot 2^{k/2}}_{=\varepsilon}$: s.t. $O(k + \log\frac{1}{\varepsilon} + \log\log n)$

Pf: $f(x) = g(x_{i_1}, \dots, x_{i_k})$ some $g: \{0,1\}^k \to \{-1,1\}$.

$L_1(g) \le 2^{k/2}$, so X $\delta 2^{k/2}$-fools g (& f). ∎

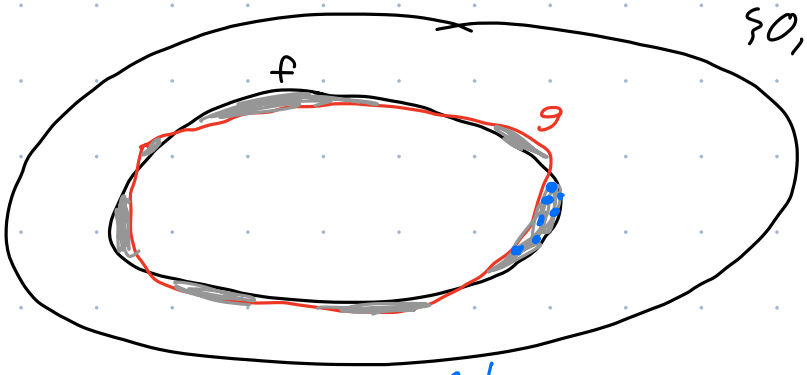
Sandwiching & Approximation

Sps have $f: \{0,1\}^n \to \{0,1\}$ you want to fool.

Sps have $g: \{0,1\}^n \to \{0,1\}$ that approximates f well: say $f(x) \neq g(x)$ for $\le \varepsilon \cdot 2^n$ inputs.

Sps X RV fools g (say X ε-fools g).

"$\cup$"? Alas, no "$\supseteq$": not necc. true X fools f.



= error $\leq \varepsilon \cdot 2^n$ points.

X: supp. on $2^{s.l.}$ # pts. Suppose s.l. $\leq n/10$,

" " $2^{n/10}$

If $2^{n/10} < \varepsilon \cdot 2^n$: could have all of X's support in error region, i.e.

So, fooling an ordinary approx. for f doesn't necc. fool f. "$\supseteq$"

"$\cup$": If f is approximable in stronger (sandwiching) sense, fooling the sand. approx. does fool f.

Def: Let $f, f_\ell, f_u : \{0,1\}^n \to \mathbb{R}$.
f is δ-sandwiched by (f_ℓ, f_u) if

1) $f_\ell(x) \leq f(x) \leq f_u(x) \quad \forall\, x \in \{0,1\}^n$, &

2) $\mathop{\mathbb{E}}_{x\sim\mathcal{U}}\left[f_u(x)-f_\ell(x)\right]\le\delta$.

Sandwiching lemma: Sps $f:\{0,1\}^n\to\mathbb{R}$ is

δ-sand. by (f_ℓ, f_u), & sps X (r.v. over $\{0,1\}^n$)

ε-fools f_ℓ

ε-fools f_u.

Then X $(\varepsilon+\delta)$-fools f.

Pf:
$$\mathop{\mathbb{E}}_{X}[f(X)] \le \mathop{\mathbb{E}}_{X}[f_u(X)]$$
$$\le \mathop{\mathbb{E}}_{\mathcal{U}}[f_u(\mathcal{U})]+\varepsilon$$
$$\le \mathop{\mathbb{E}}_{\mathcal{U}}[f(\mathcal{U})]+\varepsilon+\delta$$

Same arg for
$$\mathop{\mathbb{E}}_{X}[f(X)] \ge \dots \ge \mathop{\mathbb{E}}_{\mathcal{U}}[f(\mathcal{U})]-\varepsilon-\delta.$$

Cor: (sandwiching polys $\Rightarrow$ PRG)

A fn $f:\{0,1\}^n\to\mathbb{R}$ is ε-fooled by any k-wise indep dist X if there exist "ε-sandwiching" real polys $q_u, q_\ell:\{0,1\}^n\to\mathbb{R}$ of deg k s.t. 1), 2) hold.

Will be useful!

End of basic Fourier stuff

"easy" applic. to PRG.

Break (till 2:33)

Fooling $\mathbb{F}_2$ polys (DEG_d)

Note: real polys, deg-d:
0-fooled by d-wise indep. ($d \log n$ s.l.)

Fooling $DEG_d \supseteq \mathbb{F}_2$-polys of deg d:
very different!

Let $X = (X_1, \ldots, X_n)$ X: $X_1 = U_1$
$\vdots$
$X_{n-1} = U_{n-1}$
$X_n = U_1 \oplus \ldots \oplus U_{n-1}$

s.l. $X = n-1$
X is $(n-1)$-wise indep.

$Par_{[n]} = 0$ on X can't fool $PAR_{[n]} \in DEG_1$: every .

→ fails to fool DEG_1.

Motiv.: Why try to fool DEG_d?

Here's a reason:

Claim: ε-PRG against DEG_d for $d = (\log n)^{\omega(1)} \Rightarrow$ 3ε-PRG against $AC^0(\oplus)$ = all poly(n)-size, $O(1)$-depth $\wedge/\vee/\neg/\oplus$ ckts.

Pf: Let $G: \{0,1\}^s \to \{0,1\}^n$ be ε-PRG against DEG_d.

Fact: For any $O(1)$-depth, poly(n) size ckt C, + there's a dist. P over deg-(polylog(n)) $\mathbb{F}_2$ polynomials s.t.

$$\forall z \in \mathbb{F}_2^n, \quad \Pr_{p \sim P}[p(z) = C(z)] \geq 1 - \varepsilon.$$

(dist. of polynomials fools C on every fixed input).

Means

$$\Pr_{U_s}[C(G(U_s)) = 1] \approx_\varepsilon \Pr_{U_s, p \sim P}[p(G(U_s)) = 1]$$

G is ε-PRG for DEG_d, + $d >$ deg of polys in P, so

$$\Pr_{U_s, p \sim P}[p(G(U_s)) = 1] \approx_\varepsilon \Pr_{U_n, p \sim P}[p(U_n) = 1].$$

Since P fools C on every input, have

$$\Pr_{U_n, P\sim\mathcal{P}}[P(U_n)=1] \approx_\varepsilon \Pr_{U_n}[C(U_n)=1].$$

So $\Pr_{U_s}[C(G(U_s))=1] \approx_{3\varepsilon} \Pr_{U_n}[C(U_n)=1]$. ∎

So we want PRGs for DEG_d.

Line of work culminated in

Thm (Viola): [Sum of d indep δ-biased RVs (over $\mathbb{F}_2$) fools DEG_d] Let $Y_1, \dots, Y_d$ be indep over $\mathbb{F}_2^n$, where $\delta \le \frac{1}{2}$.

Then $Y := Y_1 + \dots + Y_d$ (over $\mathbb{F}_2$)

$$4\left(\frac{\delta}{2}\right)^{\frac{1}{2^{d-1}}} \text{-fools } DEG_d.$$

Take $\varepsilon =$: get a PRG with s.l.

$$O(d \cdot \log(n/\delta)) = O(d\cdot\log n + d\cdot 2^d \cdot \log\tfrac{1}{\varepsilon}).$$

Huh? Why would summing indep δ-biased RVs be good idea?

Obs: Let $Y_1, \dots, Y_d$ be indep δ-biased RVs over $\mathbb{F}_2^n$.

Then $Y := Y_1 + \cdots + Y_d$ is δ^d-biased.

Pf: Let $\emptyset \neq S \subseteq [n]$.

$$\left| \mathop{\mathbb{E}}_{Y}\left[\chi_S\left(\sum_{i=1}^{d} Y_i\right)\right] \right| = \left| \mathop{\mathbb{E}}\left[(-1)^{\sum_{j\in S}\sum_{i=1}^{d} Y_{i,j}}\right] \right|$$

$$= \left| \mathop{\mathbb{E}}\left[(-1)^{\sum_{i=1}^{d}\sum_{j\in S} Y_{i,j}}\right] \right|$$

$$\overset{(\text{indep})}{=} \left| \prod_{i=1}^{d} \mathop{\mathbb{E}}_{Y}\left[\chi_S(Y_i)\right] \right| \leq \delta^d.$$

Viola: also fools higher-deg polys.

Hi-level strat: show if can fool DEG_{d-1}, can add one more biased RV + fool DEG_d (with worse params).

Key Lemma: Sps W fools DEG_{i-1} with error γ, + sps Y is a δ-biased RV indep. of W. Then $W+Y$ $(\sqrt{2\gamma} + \frac{\delta}{2})$-fools DEG_i.

Pf of thm using Key Lemma: By def of δ-bias,

Y_1 $\delta/2$ - fools DEG_1. Let $\varepsilon_1 = \delta/2$.

Let $\varepsilon_{i+1} = \sqrt{2\varepsilon_i} + \delta/2$. By KL,

$Y_1 + \dots + Y_d$ ε_d - fools DEG_d. $\delta \le \frac{1}{2}$, so

$$\varepsilon_{i+1} \le \sqrt{2\varepsilon_i} + \sqrt{\delta/2}/2 \underset{\delta/2 \le \varepsilon_i}{\le} \left(\sqrt{2} + \tfrac{1}{2}\right)\sqrt{\varepsilon_i} \le 2\sqrt{\varepsilon_i}.$$

So $\varepsilon_2 \le 2\left(\delta/2\right)^{\frac{1}{2}}$

$$\varepsilon_3 \le 2^{1+\frac{1}{2}} \cdot \left(\tfrac{\delta}{2}\right)^{\frac{1}{4}}$$

$$\varepsilon_4 \le 2^{1+\frac{1}{2}+\frac{1}{4}} \cdot \left(\delta/2\right)^{1/8}$$

$$\vdots$$

$$\varepsilon_d \le 2^{1+\frac{1}{2}+\dots+\frac{1}{2^{d-2}}} \cdot \left(\frac{\delta}{2}\right)^{\frac{1}{2^{d-1}}} < 4\left(\frac{\delta}{2}\right)^{\frac{1}{2^{d-1}}}.$$

Job: Key lemma.

Case analysis dep. on "imbalance" of the $f \in DEG_i$ being fooled.

Def: For $f: \mathbb{F}_2^n \to \mathbb{F}_2$, define

$$\text{imbal}(f) = \left| \mathop{\mathbb{E}}_{u} \left[(-1)^{f(u)}\right] \right| = 2\left|\mathbb{E}[f] - \tfrac{1}{2}\right|$$

$$\in [0,1]$$

Intuition: • if f has $imbal(f)$ large, turns out W already fools f not too badly;

• if $imbal(f)$ small: analysis like corr bd: squaring of correl., derivs, etc.

---

2 lemmas:

L1 (imbal. case): Suppose W γ-fools DEG_{i-1}. Then W fools any $f \in DEG_i$ with error $\frac{\gamma}{imbal(f)}$.

L2 (bal. case): Sps W γ-fools DEG_{i-1}. Let Y be indep. of W, Y is δ-biased. Then

$W+Y$ $\left(imbal(f) + \sqrt{\gamma/2} + \frac{\delta}{2}\right)$-fools any $f \in DEG_i$.

Notation: $f^{+y}(x)$ means $f(x+y)$

Pf of KL using L1 + L2:

Fix any $f \in DEG_i$. Fix any outcome of Y.

The fn $f^{+Y}(x) = f(Y+x)$ is a deg-i poly in $x_1, \ldots, x_n$, + $imbal(f^{+Y}) = imbal(f)$

So by L1, $W+Y$ fools f with error $\frac{\gamma}{imbal(f)}$.

And by L2,

W+Y $(\text{imbal}(f) + \sqrt{\gamma/2} + \frac{\delta}{2})$-fools f.

Hence W+Y

$$\min\left\{\frac{\gamma}{\text{imbal}(f)}, (\text{imbal}(f) + \sqrt{\gamma/2} + \frac{\delta}{2})\right\}\text{-fools } f.$$

$$\leq \sqrt{2\gamma} + \frac{\delta}{2}$$

$(\text{imbal}(f) \leq \sqrt{\gamma/2})$

$\geq$

■

To show: L1 $\Rightarrow$ L2.

Both involve deriv's.

Recall: for $f: \mathbb{F}_2^n \to \mathbb{F}_2$, $y \in \mathbb{F}_2^n$,

the directional derivative $\partial_y f$ is

$\partial_y f: \mathbb{F}_2^n \to \mathbb{F}_2$,

$$\partial_y f(x) = f^{+y}(x) + f(x)$$
$$= f(y+x) + f(x).$$

Saw: if f is deg i, then

$\forall y$, $\partial_y f$ is deg $\leq (i-1)$.

Pf of L1:

L1 (imbal. case): Suppose W γ-fools DEG_{i-1}. Then W fools any $f \in DEG_i$ with error $\frac{\gamma}{imbal(f)}$.

To show: $imbal(f) \cdot \left| \mathbb{E}[(-1)^{f(W)}] - \mathbb{E}[(-1)^{f(U')}] \right| \leq 2\gamma$,

where U' uniform.

Let U indep, uniform. Have

$$= \left| \mathbb{E}\left[(-1)^{f(W)+f(U)}\right] - \mathbb{E}\left[(-1)^{f(U')+f(U)}\right] \right|$$

($\partial_U f(W) = (\deg i-1)$ poly in W; $\partial_U f(U')$, same deg $i-1$ poly in U')

$$= \left| \mathbb{E}\left[(-1)^{f(W)+f(W+U)}\right] - \mathbb{E}\left[(-1)^{f(U')+f(U'+U)}\right] \right|$$

$\leq 2\gamma$, bc for any fixing of U, $\partial_U f$ is deg-$(i-1)$, hence γ-fooled by W. ∎ End of L1 pf"

Next time: pf of L2, which finishes pf of Viola's thm.

L2 (bal. case): Sps W γ-fools DEG_{i-1}. Let Y be indep. of W, Y is δ-biased. Then $W+Y$ $\left(imbal(f) + \sqrt{\gamma/2} + \frac{\delta}{2}\right)$-fools any $f \in DEG_i$.

Enjoy Spring Break!