Last time:

- finish pf of Viola's thm ($\sum_{i=1}^{d} Y_i$ fools DEG_d) δ-biased
- tools for Braverman's thm:
  $(\log n)^{O(1)}$-wise indep. fools AC^0

  $\left(\log(s/\varepsilon)\right)^{O(d^2)}$-wise indep. ε-fools size-s, depth-d AC^0.

  - BRS poly. approx. of AC^0 (pointwise)
  - start LMN poly. approx. of AC^0 (L_2)

Today:

- finish (the Fourier-wt-under-restriction result)
- Proof of Braverman's thm: combining +
- start unit on Linear Threshold Functions (LTFs):
  basics, examples, regularity, Berry-Esseen Thm
- start (sketch of) PRG:
  $\tilde{O}(1/\varepsilon^2)$-wise independence ε-fools LTFs.

Scribes: Patrick, Szymon

Questions?

To do: finish LMN approx.

(L2): For any $f: \{\pm 1\}^n \to \{\pm 1\}$, any $p \le \frac{1}{10}$, have

$$W^{\ge t/p}(f) \le 2 \cdot \mathbb{E}_{(J,z)\sim R_p}\left[W^{\ge t}[f_{J,z}] \right].$$

Here are the steps:

Claim 1: For any $f: \{\pm 1\}^n \to \{\pm 1\}$, any $S \subseteq [n]$,

S J T

$$\widehat{f_{J,z}}(S) = \begin{cases} 0 & \text{if } S \not\subseteq J \\ \sum_{T \subseteq \bar{J}} \hat{f}(S \cup T) \cdot \chi_T(z) & \text{if } S \subseteq J \end{cases}$$

Claim 2: For fixed $J, S \subseteq [n]$ & unif. rand. $z \sim \{\pm 1\}^{\bar{J}}$, have

OHP

$$\mathop{\mathbb{E}}_{z \in \{\pm 1\}^{\bar{J}}}\left[\widehat{f_{J,z}}(S)\right] = \mathbb{1}[S \subseteq J]\, \hat{f}(S)$$

$$\mathop{\mathbb{E}}_{z \in \{\pm 1\}^{\bar{J}}}\left[\widehat{f_{J,z}}(S)^2\right] = \mathbb{1}[S \subseteq J] \cdot \sum_{T \subseteq \bar{J}} \hat{f}(S \cup T)^2$$

Claim 3: For $(J, z) \sim R_p$, have (each $i \in [n]$ is in J w.p. p, $z \sim \{\pm 1\}^{\bar{J}}$)

OHP

$$\mathop{\mathbb{E}}_{(J,z) \sim R_p}\left[\widehat{f_{J,z}}(S)\right] = p^{|S|} \cdot \hat{f}(S),$$

$$\mathop{\mathbb{E}}_{(J,z) \sim R_p}\left[\widehat{f_{J,z}}(S)^2\right] = \sum_{U \subseteq [n]} \hat{f}(U)^2 \cdot \Pr_J[U \cap J = S]$$

Claim 4: OHP

$$\mathop{\mathbb{E}}_{(J,z) \sim R_p}\left[W^{\geq k}(f_{J,z})\right] = \sum_{r \geq k} W^r(f) \cdot \Pr\left[\mathrm{Bin}(r, p) \geq k\right]$$

Let's use this to conclude: want to show

For any $f: \{\pm 1\}^n \to \{\pm 1\}$, any $p \leq \frac{1}{10}$,

have

$$W^{\geq t/p}(f) \leq 2 \cdot \mathop{\mathbb{E}}_{(J,z) \sim R_p}\left[W^{\geq t}[f_{J,z}]\right].$$

Claim 4 gives

$$\underset{(J,z)\sim R_p}{\mathbb{E}}\left[W^{\geq k}(f_{J,z})\right] = \sum_{r \geq k} W^r(f) \cdot \Pr\left[\mathrm{Bin}(r,p) \geq k\right]$$

$$\geq \sum_{r \geq \frac{k}{p}} W^r(f) \cdot \underbrace{\Pr\left[\mathrm{Bin}(r,p) \geq k\right]}_{\geq \frac{1}{2}}$$

since $k \leq k/p$. For each $r \geq k/p$, have

(bin. dist. fact.) So

$$\sum_{r \geq \frac{k}{p}} W^r(f) \cdot \Pr\left[\mathrm{Bin}(r,p) \geq k\right] \geq \frac{1}{2} \cdot \sum_{r \geq k/p} W^r(f)$$

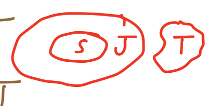
$$= \frac{1}{2} \cdot W^{\geq k/p}(f).$$

$t \leftarrow k$

Done! (modulo proving C1-C4)

Claim 1: For any $f : \{\pm 1\}^n \to \{\pm 1\}$, any $S \subseteq [n]$,

$$\widehat{f_{J,z}}(S) = \begin{cases} 0 & \text{if } S \not\subseteq J \\ \sum_{T \subseteq \bar{J}} \hat{f}(S \cup T) \cdot \chi_T(z) & \text{if } S \subseteq J \end{cases}$$



Pf:

Sps $S \not\subseteq J$. Some $x_i \in S$, $x_i \notin J$.

View $f_{J,z}$ as n-var fn, but it's a J-junta: only dep. on vars in J. i.e.

$$f_{J,z}(x) = f(x_J, z)$$

∀ S cont. irrel. var. for $f_{J,z}$, so

$\mathbb{E}[f \cdot \chi_S] = 0 = \widehat{f_{J,z}}(S)$. So $\widehat{f_{J,z}}(S) = 0$ if $S \not\subseteq J$.

Sps $S \subseteq J$. Have

$R = S \cup T$

$$\underbrace{f_{J,z}(x_J, z)}_{= f_{J,z}(x)} = \sum_{R \subseteq [n]} \hat{f}(R) \cdot \chi_R(x_J, z)$$

$$= \sum_{S \subseteq J} \sum_{T \subseteq \bar{J}} \hat{f}(S \cup T) \cdot \chi_S(x_J) \cdot \chi_T(z)$$

$$= \sum_{S \subseteq J} \chi_S(x_J) \cdot \overbrace{\left(\sum_{T \subseteq \bar{J}} \hat{f}(S \cup T)\, \chi_T(z) \right)}^{\text{this must } = \widehat{f_{J,z}}(S)} \qquad \blacksquare$$

C2, C3, C4: Official HW Problems

Now: the $AC^0_{s,d}$ PRG! Using

Thm (LMN): Let $f \in AC^0_{s,d}$. There's a real poly p_2, of deg $O((\log \frac{s}{\varepsilon})^d)$, s.t.

$$\mathbb{E}_{\mathcal{U}}\left[(f(\mathcal{U}) - p_2(\mathcal{U}))^2 \right] \le \varepsilon.$$

+

Lemma (BRS): Let $f \in AC^0_{s,d}$. Let $\mathcal{D}$ be any dist. over $\{0,1\}^n$. There's a real poly p s.t.

$$\Pr_{x \sim \mathcal{D}}[p(x) = f(x)] \ge 1 - \varepsilon, \text{ where}$$

(i) $\deg(p) \le (\log \frac{s}{\varepsilon})^{O(d)}$, +

(ii) $\forall x \in \{0,1\}^n$, $|p(x)| \le \exp\left((\log \frac{s}{\varepsilon})^{O(d)} \right)$.

(*) More info abt BRS approx: augment w/ new obs: the "error region" of p is computed by an AC^0 ckt.

Extended BRS:

Lemma BRS Let $f \in AC^0_{s,d}$.
Let $\mathcal{D}$ be any dist. over $\{0,1\}^n$.
There's a real poly p s.t.

$$\Pr_{x \sim \mathcal{D}}[p(x) = f(x)] \geq 1 - \varepsilon$$

+ a ckt E, of size poly(s) + depth $d + O(1)$, s.t.

(i) $\deg(p) \leq (\log \frac{s}{\varepsilon})^{O(d)}$, +

(ii) $\forall x \in \{0,1\}^n, \quad |p(x)| \leq \exp((\log \frac{s}{\varepsilon})^{O(d)})$.

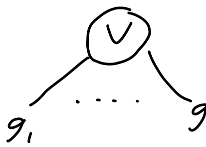
(iii) $E(x) = 0 \Rightarrow p(x) = f(x)$ (i.e. $p(x) \neq f(x) \Rightarrow E(x) = 1$), +

$$\Pr_{x \sim \mathcal{D}}[E(x) = 1] \leq \varepsilon.$$

Pf: Idea: E checks "did anything go wrong" in building the poly p (anywhere along the way of building p), outputs 1 if so.

Need to describe E, show it's in $AC^0_{\text{poly}(s), d+O(1)}$.

Consider any fixed OR gate in ckt for f:



some $t \leq s$. In the poly we used

$$1 - \prod_{i=1}^{\text{polylog}(t/\varepsilon)} \left(1 - \sum_{j \in S_i} g_j\right)$$

for diff. sets $S_i \subseteq [t]$.

This poly wrong exactly when

① at least one of $g_1, \dots, g_s$ is 1, but

② each set S_i has either no 1's or ≥ 2 of the 1's in $g_1, \dots, g_t$.

This is checkable in const depth, e.g.

$$\bigvee_{1 \le a < b \le t} g_a \wedge g_b$$

Do this for each gate, OR all results; that's E.

So, if nothing goes wrong at any gate, $E(x) = 0$ & $p(x) = f(x)$.

if something went wrong at some gate, $E(x) = 1$. Have $\Pr_{x \sim \mathcal{D}}[E(x) = 1] \le \varepsilon$ from old analysis. $\blacksquare$

(**) Refined sandwiching goal:

Recall

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:

1) $q_\ell(x) \le f(x) \le q_u(x)$, $\forall$

2) $\underset{x \sim \mathcal{U}}{\mathbb{E}}[g_u(x) - g_\ell(x)] \le \varepsilon$.

Small obs: since AC^0 closed under neg., to give g_u, g_ℓ, enough to just give g_ℓ s.t.

$$g_\ell \le f \quad \& \quad \mathbb{E}[f - g_\ell] \le \varepsilon/2.$$

$\left(1 - g_\ell \text{ will be } g_u\right)$.

<u>Bigger obs:</u> It's enough to give a lower sand. poly g_ℓ which

1) can depend on the partic. k-wise ind. $\mathcal{D}$, &
2) lower sand. f', where f' is close to f both under $\mathcal{D}$ & under $\mathcal{U}$:

<u>Lemma:</u> Sps, for every <u>k-wise ind. $\mathcal{D}$</u>, have a Bool fn f' & a <u>deg-k poly g_ℓ</u> s.t.

ⓐ $\underset{x \sim \mathcal{D}}{\Pr}[f(x) \ne f'(x)] \le \frac{\varepsilon}{3}$, & $\underset{x \sim \mathcal{U}}{\Pr}[f(x) \ne f'(x)] \le \frac{\varepsilon}{3}$,

ⓑ g_ℓ lower sand. f': $g_\ell \le f'$, & $\underline{\underset{x \sim \mathcal{U}}{\mathbb{E}}[f'(x) - g_\ell(x)] \le \frac{\varepsilon}{3}}$.

Then $\mathbb{E}[f(\mathcal{U})] - \underset{x \sim \mathcal{D}}{\mathbb{E}}[f(x)] \le \varepsilon$. (Comb. this w/ g_u version: this means $\mathcal{D}$ ε-fools f.)

<u>Pf:</u>

$$\underset{x \sim \mathcal{D}}{\mathbb{E}}[f(x)] \ge \underset{x \sim \mathcal{D}}{\mathbb{E}}[f'(x)] - \varepsilon/3 \qquad (a)$$

$$\ge \underset{x \sim \mathcal{D}}{\mathbb{E}}[g_\ell(x)] - \varepsilon/3 \qquad (g \le f' \text{ everywhere})$$

$$= \mathop{\mathbb{E}}_{x\sim\mathcal{U}}[g_\ell(x)] - \varepsilon/3 \qquad (\mathcal{D}\ k\text{-wise indep}, \deg g_\ell \le k)$$

$$\geq \mathop{\mathbb{E}}_{x\sim\mathcal{U}}[f'(x)] - 2\varepsilon/3 \qquad (b)$$

$$\geq \mathop{\mathbb{E}}_{x\sim\mathcal{U}}[f(x)] - \varepsilon.$$

So Suff. to show:

<u>Lem:</u> Let $f \in AC^0_{s,d}$, let $k = (O(\log \frac{s}{\varepsilon}))^{O(d^2)}$.

Let $\mathcal{D}$ be any k-wise indep. dist.

Then there is a Bool. fn. f', a deg-k poly g_ℓ ($= p$)

s.t. (a), (b) both hold.

<u>Pf:</u> • Apply BRS approx. to f using dist $\frac{1}{2}(\mathcal{D} + \mathcal{U})$, error param. $\varepsilon/8$.

Gives a poly p_0 s.t.

$$\Pr_{x\sim\mathcal{D}}[p_0(x) \neq f(x)] \leq \frac{\varepsilon}{4}, \quad \Pr_{x\sim\mathcal{U}}[p_0(x) \neq f(x)] \leq \frac{\varepsilon}{4},$$

+ a <u>poly(s)-size, depth-$(d+O(1))$</u> ckt E s.t.

$$f(x) \neq p_0(x) \Rightarrow E(x) = 1, \quad + \Pr_{x\sim\mathcal{D} \text{ or } \mathcal{U}}[E(x)=1] \leq \varepsilon/4.$$

• Apply LMN on E: let $p_{E,2}$ be the poly of deg $(\log(s/\delta))^{O(d)}$ s.t.

(we'll choose δ soon)

$$\mathop{\mathbb{E}}_{u \sim \mathcal{U}}\left[(E(u) - p_{E,z}(u))^2 \right] \le \delta.$$

Set

$f' = f \vee E$, $\quad q = p_0(1 - p_{E,z})$,

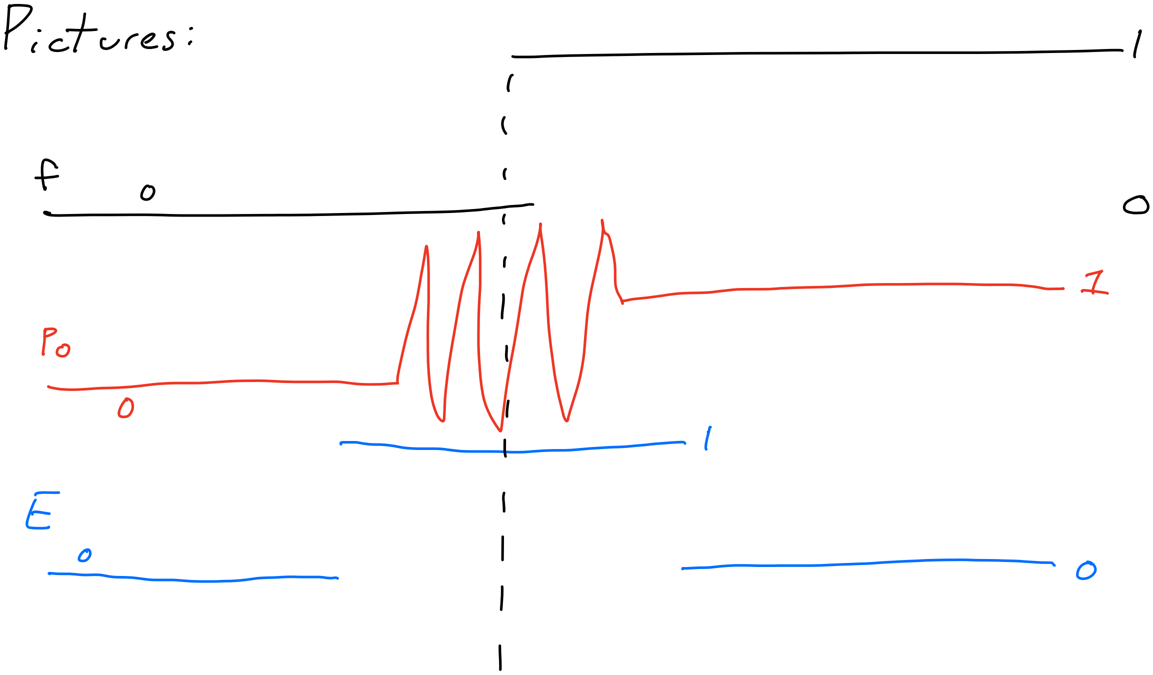
final $p = q_\ell = 1 - (1-q)^2$.

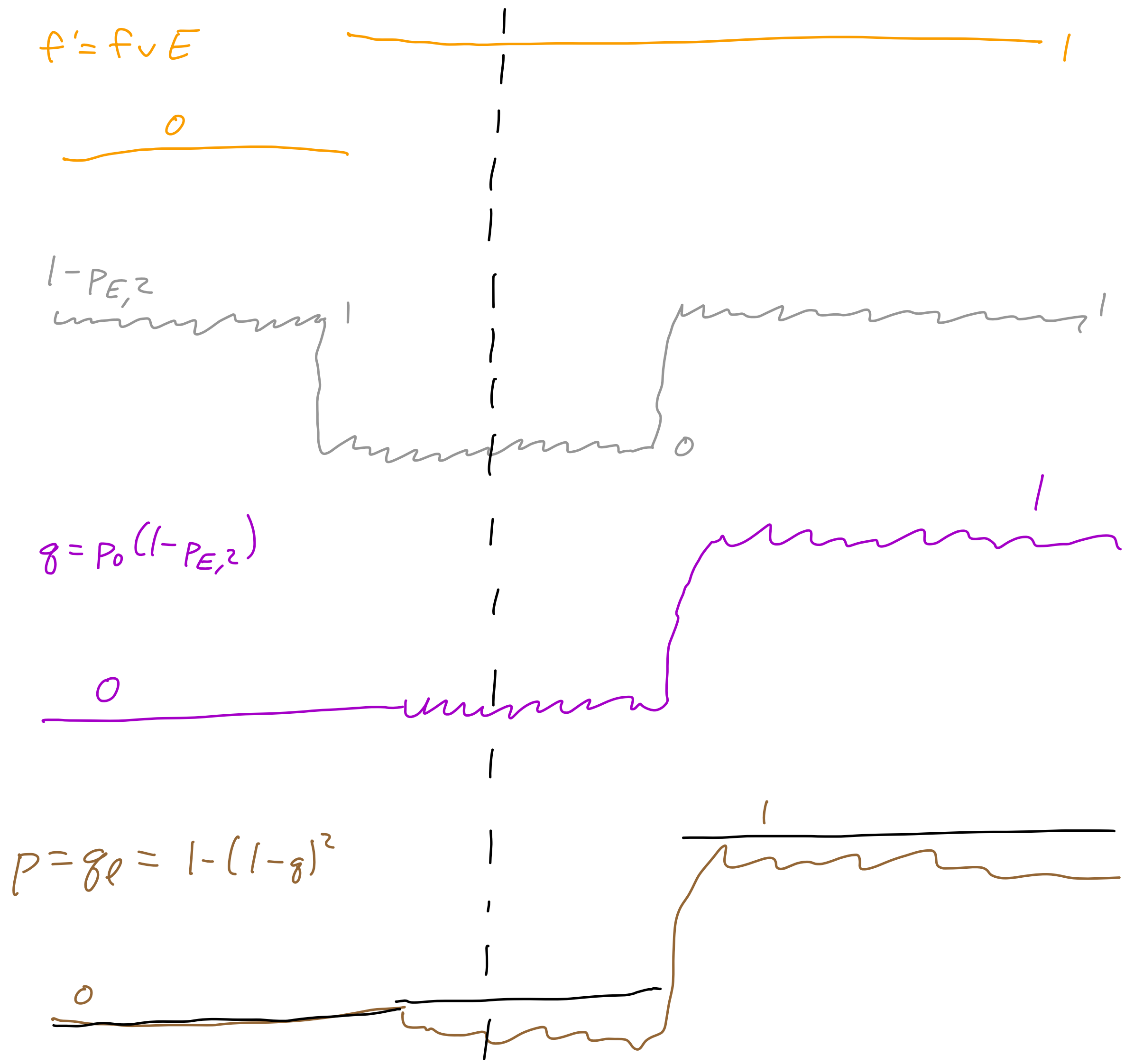
|Break|

Intuition:

- f' close to f b/c error region E is small
- p_0 may make wild errors on f' when $E(x) = 1$; mult. by $1 - p_{E,z}$ "tames" these errors, but $q = p_0(1 - p_{E,z})$ may not be a lower sandwicher when $f' = 1$
- Taking $p = 1 - (1-q)^2$ makes it always ≤ 1.

Pictures:





Pf/details: Need (a) + (b)

(a): $f' \neq f$ only if $E = 1$ +
under $\mathcal{D}$ or $\mathcal{U}$, have $\Pr[E=1] \leq \varepsilon/4$.
(a) ✓

Need (b): $p = q_\ell = 1-(1-q)^2$ is lower sand. for f'.

Claim 1: if $\boxed{f'(x) = 0 \text{ then } q(x) = 0.}$

$f' = f \vee E$, $g = p_0(1 - p_{E,2})$

Final $p = g_\ell = 1 - (1-g)^2$.

Pf: if $f' = f \vee E = 0$,

have $E = 0$, no mist., so

$p_0(x) = f(x) = 0$ & so $g(x) = 0$.

Claim 2: $\|f' - g\|_2 \le \sqrt{\varepsilon/4} + \exp(\log(s/\varepsilon))^{O(d)} \cdot \sqrt{\delta}$,

which is $\le \sqrt{\varepsilon/3}$ by taking

$$\boxed{\delta = \varepsilon \cdot \exp\left(-\log(s/\varepsilon)^{O(d)}\right).}$$

Recall: for fns $a, b : \{\pm 1\}^n \to \mathbb{R}$,

$$\|a - b\|_2 = \mathbb{E}_{\mathcal{U}}\left[(a-b)^2\right]^{\frac{1}{2}}.$$

Pf: $\triangle$ ineq:

$$\|f' - g\|_2 \le \|f' - p_0(1-E)\|_2 + \|p_0(1-E) - g\|_2 .$$

1st: $\le \sqrt{\Pr_{\mathcal{U}}[E = 1]} \le \sqrt{\varepsilon/4}$

2nd: write $p_0(1-E) - g = p_0(p_{E,2} - E)$.

Using our ptwise bd on p_0, have $\underline{\max_x |p_0(x)| \le \exp(\log(\tfrac{s}{\varepsilon})^{O(d)})}$,

so get

LMN bounded this!

$$\|p_0(1-E) - g\|_2 \le \exp\left(\log(\tfrac{s}{\varepsilon})^{O(d)}\right) \cdot \|p_{E,2} - E\|_2$$

$$\le \exp\left(\log(\tfrac{s}{\varepsilon})^{O(d)}\right) \cdot \sqrt{\delta}$$

$\blacksquare$ (Claim 2)

(b): $p = q_\ell = 1-(1-q)^2$ is lower sand. for f':

Have
$p \le f'$ pointwise, b/c if $f'=0$, then
$q=0$ so $p(x)=0$ $\quad 0 \le 0$:)

if $f'(x)=1$, then

$$\underline{f'(x) - p(x)} = (1-q(x))^2 = \underline{(f'(x)-q(x))^2}.$$

So $$\mathop{\mathbb{E}}_{x\sim\mu}[f'(x)-p(x)] = \mathbb{E}[|f'(x)-p(x)|]$$
$$\le \mathbb{E}[(f'(u)-q(u))^2]$$
$$\le \varepsilon/3.$$

---

deg p ?

$f' = f \vee E$, $\quad q = p_0(1-p_{E,2})$

Final $p = q_\ell = 1-(1-q)^2$.

$$\le 2\cdot(\underbrace{\deg p_0}_{\substack{\log(s/\varepsilon)^{O(d)} \\ \text{BRS}}} + \underbrace{\deg p_{E,2}}_{\text{LMN}})$$

LMN

$\log(s/\delta)^{O(d)}$

$= \left(\left(\log\left(\frac{s}{\varepsilon}\right)\right)^{O(d)}\right)^{O(d)}$

$= (\log(s/\varepsilon))^{O(d^2)}$ $\blacksquare$

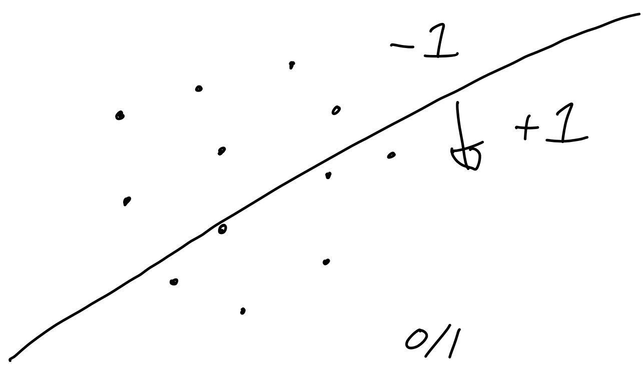
Braverman's thm: done!

Next unit: LTFs

linear threshold functions / halfspaces.

$f: \{\pm 1\}^n \to \{\pm 1\}$ is an LTF if
$\{0,1\}^n$ $\quad$ $\forall x \in \{\pm 1\}^n$,

$f(x) = \mathrm{sign}(w \cdot x - \theta)$ for some $w \in \mathbb{R}^n$, $\theta \in \mathbb{R}$.



0/1

$x_1 \vee \dots \vee x_k$ $\qquad$ $\mathrm{sign}(x_1 + \dots + x_k - \frac{1}{2})$

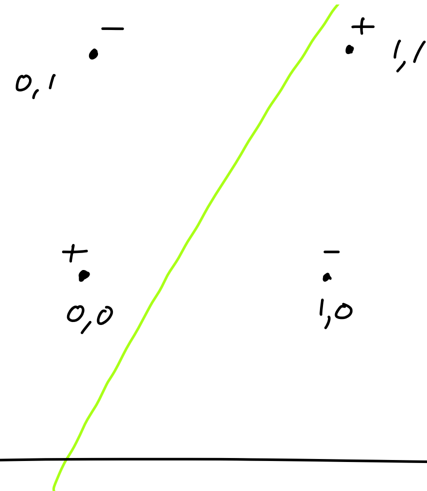
±1

$\mathrm{MAJ}(x_1, \dots, x_k) = \mathrm{sign}\left(\sum_{i=1}^{k} x_k\right)$

0/1

$\mathrm{sign}(2^n x_1 - 2^{n-1} x_2 + 2^{n-2} x_3 - \dots)$

$PAR(x_1, x_2)$
not computed by an LTF.
(LB's: easy)



We'll focus on PRGs + det approx. count. for LTFs.

Q: can we, in poly(n) time, given an LTF (w, θ), output $|f^{-1}(1)|$ exactly?
$f(x)$

No: #P-hard to do exact counting.

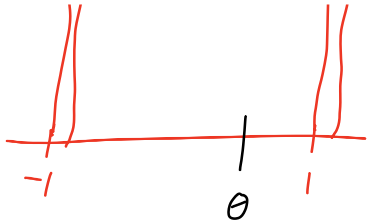
What is $|f^{-1}(1)|$ for f an LTF?

The LTF $\text{sign}(w \cdot x - \theta)$:

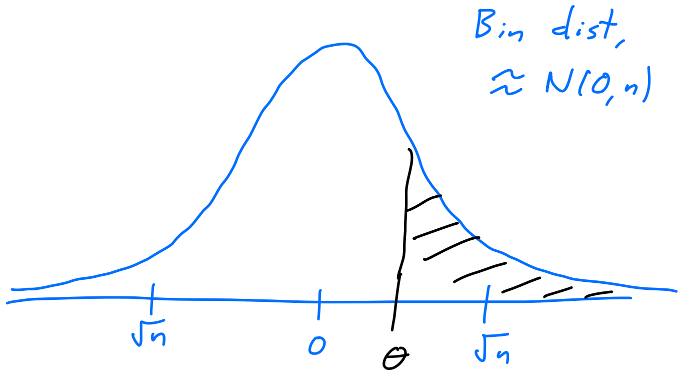
2^n values of $w \cdot x$ as x ranges over $\{\pm 1\}^n$: a discrete dist. over $\mathbb{R}$.

Ex: dist of $w \cdot x$

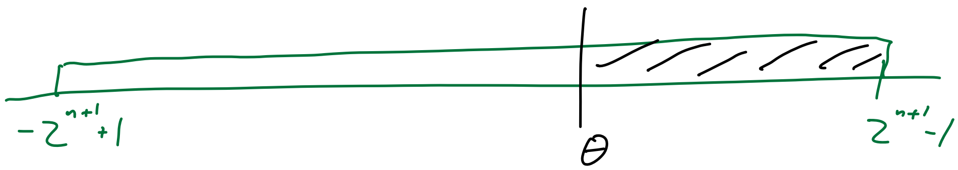
$w \cdot x = x_1$:



$w \cdot x = X_1 + \cdots + X_n$



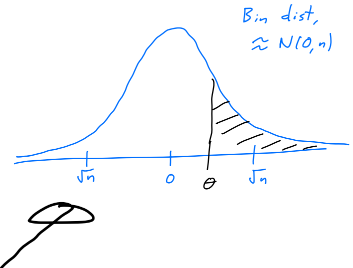
$$w \cdot x = \sum_{i=1}^{n} 2^i x_i$$



$$w \cdot x = \sum_{j=1}^{n} j^{\log^2 j} \cdot x_j$$

?

Next time:



is the nicest of these;

"regularity" of an LTF: how much it looks like