Last time: LTFs.

- regularity, Berry-Esseen Thm
- PRG: $\tilde{O}(1/\varepsilon^2)$-wise independence ε-fools LTFs.
  - $\tilde{O}(1/\varepsilon^2)$-wise indep. ε-fools ε-regular LTFs
    via low-deg univariate poly. approx. to sign(t)
  - beyond regular LTFs: "critical index", junta approx.

Today: quick high-level sketch of

- Det approx counting for LTFs (relative error)

  +

  Det approx counting for PTFs (absolute error)

- Nisan-Wigderson PRG: generic way to get PRGs for $\mathcal{C}$ from average-case LBs for (related) $\mathcal{C}'$

Scribe: Jiaze

Questions?

Next week: presentations by

- Yizhi
- Szymon + Sam
- Ashvin/Mark/Walt

arrive on time - 1:10 sharp start!

---

① Det. approx. count. (rel. error!) for LTFs

↳ input: $w_1, \dots, w_n, \theta, \varepsilon > 0$

output: $\hat{N}$ s.t.

$$N \le \hat{N} \le (1+\varepsilon)N,$$

where $N = \#\{x : f(x) = \mathrm{sign}(w \cdot x - \theta)\}$.

1st rand. alg: 1999.

Sketch of det alg:

$w_i, \theta \in \mathbb{Z}$

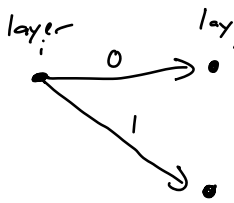
$W = \max\{|w_1|, \ldots, |w_n|, |\theta|\}$

Thm: There's a $\mathrm{poly}(n, \log W, \frac{1}{\varepsilon})$-time det alg solving

Idea: • approx the CTF using a branching program
• use standard DP to exactly count # s.a. of .

Def: An (S, T)-branching program (S = width) is a layered digraph w/ $0, 1, \ldots, T$ as "layers", $\leq S$ "states" (vertices) / layer.

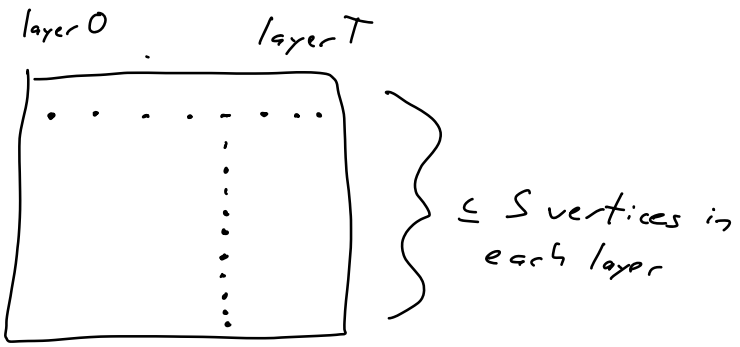
Layer 0: single source vtx s

Each layer-i node: 

(i^{th} var x_i is 0 or 1)

Each layer-T vtx labeled 0 (rej) or 1 (acc).

Computes a fn $f: \{0,1\}^T \to \{0,1\}$ in obvious way.

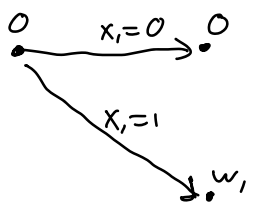


Conn. w/ LTFs: say $w_1, \ldots, w_n, \theta \geq 0$ in $\mathbb{Z}$

Let $W = \sum_{i=1}^{n} w_i$.

f is computed by a $(W+1, n)$-BP.

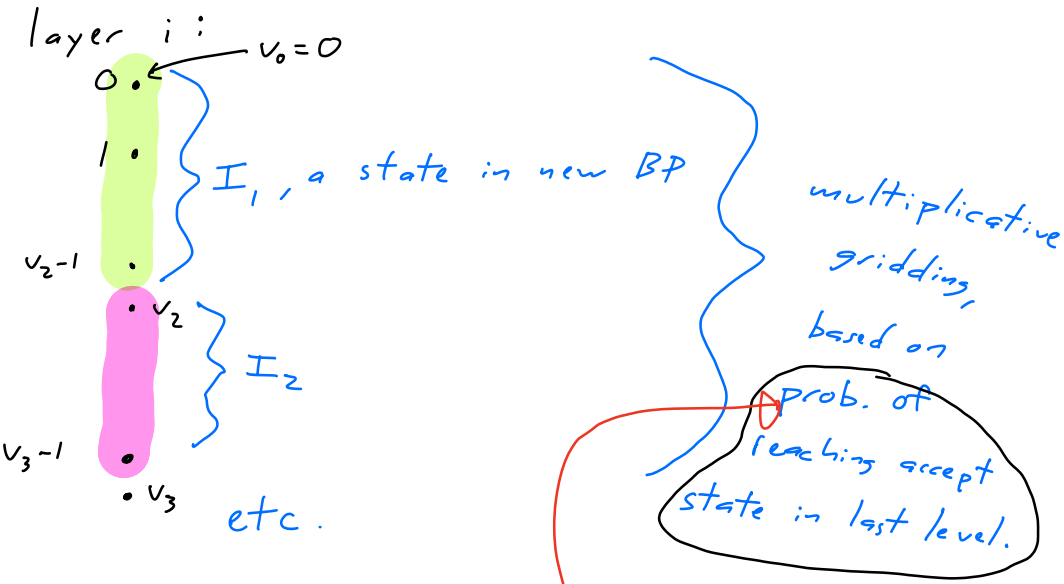
each state in layer j corr. to poss. int. value of $w_1 x_1 + \cdots + w_j x_j$



Fact: can exactly compute # s.a. of an (S,T)-BP in $\text{poly}(S,T)$ time (OP).

Key idea: approx. the $(W+1, n)$-BP for our LTF f with a $(\text{poly}\log(W), n+1)$-BP. } use OP to count # s.a. exactly.

states of states of orig. BP. correspond to subsets of

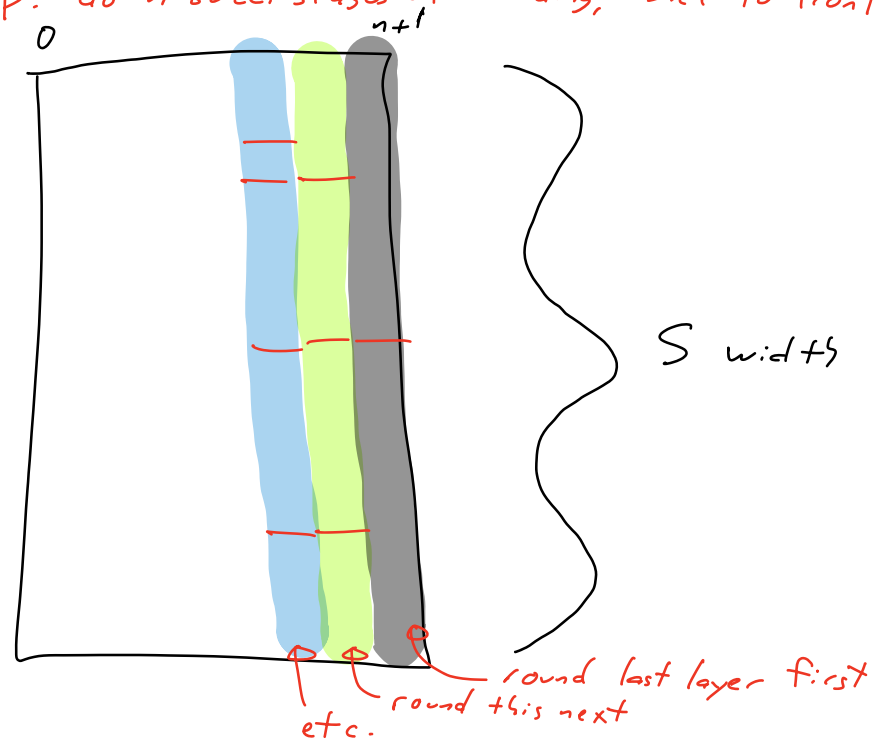


W.

This is "rounding" the BP.

Problem: computing/approx. is a problem of approx. counting # s.a. of an LTF!

Sol: OP: do n succ. stages of rounding, "back to front"



PTFs?

Deg-d PTF: Bool fn $f: \{-1,1\}^n \to \{-1,1\}$,

$f(x) = \text{sign}(p(x))$ p a deg-d real poly.

PRGs: seed length

for deg-d PTFs:

- $(d/\varepsilon)^{O(d)} \cdot \log n$ (MZ)

  approx. count. in $n^{(d/\varepsilon)^{O(d)}}$ time

- $O_d(1) \cdot \text{poly}(1/\varepsilon) \cdot \log n$ s.t.

  approx. count. in $n^{O_d(1) \cdot \text{poly}(1/\varepsilon)}$ time.

input size of deg-d PTF: $\approx n^d$

Can do $O_{d,\varepsilon}(1) \cdot n^{O(d)}$-time det. approx. counting for deg-d PTFs

(poly time in input length, for any const d.)

Deg $d=2$, some ingred:

- ext. of BE thm:

  → reg. lin. form in indep RV's
  "behaves like a Gaussian".

  → "Invariance Principle" of M,O,O:
  extension of BE to low-deg polynomials

$p(x)$ "regular" poly:

dist. of $p(x_1,\dots,x_n)$ vs dist of $p(g_1,\dots,g_n)$

$x \sim \{\pm 1\}^n$ $g \sim N(0,1)^n$

Leads to analyzing polys with $N(0,1)^n$ inputs...

Last topic: Nisan-Wigderson PRG

"hardness vs randomness"

NW PRG: generic PRG giving

- a PRG for a class $\mathcal{C}$ of n-var Bool fns
  from
- an avg-case l.b. against a "richer" class $\mathcal{C}'$
  of r-var Bool fns.

NW generator $G(U_1, \ldots, U_s) = n$-bit pseudorand. string

($U_1, \ldots, U_s$: true rand $\sim \{0,1\}^s$)

Works like this:

Let S be a special seq. of n subsets of $[s]$

$S = (S_1, \ldots, S_n)$ each $S_i \subseteq [s]$

$|S_1| = \ldots = |S_n| = r$.

Let $h : \{0,1\}^r \to \{0,1\}$ be "avg-case hard" for $\mathcal{C}'$

(*) $G(\underbrace{U_1, \ldots, U_s}_{s \text{ bits} \;=\; U}) = \big(h(U|_{S_1}), h(U|_{S_2}), \ldots, h(U|_{S_n}) \big)$, (n bits)

($h(U|_{S_1})$: s bits; $h(U|_{S_2})$: r bits; $h(U|_{S_n})$: r bits)

(intuition: hardness of h makes each bit of output "unpredictable")

where

$S_1, S_2, \ldots, S_n \subset [s]$ are "almost disjoint"

each pair S_i, S_j has $|S_i \cap S_j|$ very small.

$\mathcal{C}' = \mathcal{C} \circ \text{Junta}_{r,k}$: means $\{0,1\}^r \to \{0,1\}$

$\mathcal{C}' = \{ f(g_1(x), \ldots, g_n(x)) : f \in \mathcal{C}, \; g_i : \{0,1\}^r \to \{0,1\} \text{ (each is a } k\text{-junta)} \}$.

($\mathcal{C}$: class of $\{0,1\}^r \to \{0,1\}$ fns)

The thm:

Prelim.
Thm (NW): Let $\mathcal{C}$ = a class of $\{0,1\}^n \to \{0,1\}$ fns.

Let $h: \{0,1\}^r \to \{0,1\}$ be ε-hard for $\mathcal{C}' = \mathcal{C} \circ \text{Juntas}_{r,k}$.

Let $S = (S_1, \ldots, S_m)$ be an (s,r,k)-design.

Then the generator $\circledast$ (εn)-fools $\mathcal{C}$ & has seed length s.

↳ we'll define & prove existence.

Note: • need $\varepsilon \ll \frac{1}{n}$ for to say anything.
• need $s \ll n$ to be meaningful
• need $r \leq s$.

To do: • define & prove (s,r,k)-designs
• prove NW thm.

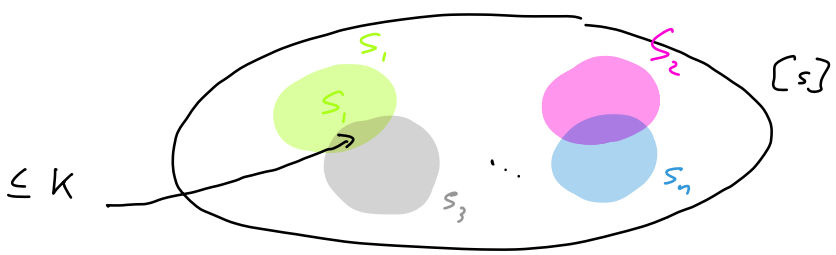
Designs

Def: A list $S = (S_1, \ldots, S_m)$ of m subsets $S_i \subset [s]$

is an (s,r,k)-design if

① $|S_i| = r \quad \forall\, i = 1, \ldots, m$, &
② $\forall\, i \neq j, \quad |S_i \cap S_j| \leq k$.

m = # sets
s = univ. size
r = size of each set
k = u.b. on overlap.



Dream: • $s \ll n$ (s = seed length)
• k very small (k big $\Rightarrow$ Juntа$_k$ powerful
$\Rightarrow$ e' powerful
$\Rightarrow$ having h be hard for e' is tough)

Tension among params:
- small $k \Rightarrow$ big s.
- def. have to have $s \geq \log n$

Need to construct design (it's part of PRG!)

Good news:

Lemma: Let $c \geq 1$. Let $s = 100c^2 \cdot \log n$.
$r = c \cdot \log n$
$k = \log n$.
Greedy alg to construct $S_1, \ldots, S_n$ sat. ① + ② works, runs in $\leq \text{poly}(n) \cdot 2^s$ time.

Pf: Greedy alg. runs in n stages: tries all $|S_i| = r$ at stage i, looking for one s.t. $|S_i \cap S_j| \leq k \ \forall j < i$.
FAILs if none exists.
Note time as claimed.
To show: succeed.
We'll show: after picking sets $S_1, \ldots, S_{i-1}$, a random $S \subset [s]$, $|S| = r$ has

$$\Pr_S\left[|S \cap S_i| > k \text{ for some } j \in [i-1]\right] < 1.$$

Follows from showing

$$\Pr_S\left[|S \cap \{1,\dots,r\}| > k\right] < \frac{1}{n}, \quad r = c\log n.$$

Note $\mathbb{E}_S\left[|S \cap \{1,\dots,c\log n\}|\right] = (c\log n)\cdot\frac{(c\log n)}{100c^2\log n}$

$$= \frac{\log n}{100}.$$

recall $k = \log n$

it's gonna work...

calc. w/ bin. coeff, or variant of CB argument for negatively corr. RVs works. ■

Ultimate Actual

Thm (NW): Let $\mathcal{C}$ = a class of $\{0,1\}^n \to \{0,1\}$ fns.

Let $h: \{0,1\}^r \to \{0,1\}$ be ε-hard for $\mathcal{C}' = \mathcal{C} \circ \text{Juntar}_{t,k}$.

Let $S = (S_1,\dots,S_m)$ be an (s,r,k)-design, where $s = 100c^2\log n$, $r = c\log n$, $k = \log n$. (these ↓ exist!) 

Then the generator ⊛ (εn)-fools $\mathcal{C}$ & has seed length s.

Applic: fool AC^0.

Cor. of: The NW gen. gives a δ-PRG for $AC^0_{M,d}$ with seed length (for $M \geq n$)

$s = \left(\log\left(M/\delta\right)\right)^{2d+O(1)}$, computable in

$\text{poly}(n) \cdot 2^s$ time.

Pf: param. setting + our earlier avg-case lbs against AC^0, using $AC^0_{M,d} \circ \text{Juntar}_{r,k}$ is contained in $AC^0_{\substack{\text{size} \\ M + n \cdot 2^k}, \substack{\text{depth} \\ d+2}}$

Pf of thm:

Key notion: "next-bit unpredictability."

Def: Let X be a RV over $\{0,1\}^n$.
Let $f: \{0,1\}^n \to \{0,1\}$, let $\varepsilon > 0$.

We say X is ε-next-bit-unpredictable for f (ε-nbu) if
for each $i \in [n]$,
for each $a \in \{0,1\}^{n-i+1}$, have

$$\left| \Pr_X\left[f(X_1, \ldots, X_{i-1}, a) = X_i\right] - \frac{1}{2} \right| \leq \varepsilon.$$

(equiv., X ε-fools $x \longmapsto f(x_1, \ldots, x_{i-1}, a) \oplus x_i$)

Pf of NW thm:

(i) NW-gen. is ε-nbu for all $f \in \mathcal{C}$.

(ii) if RV X is ε-nbu for all $f \in \mathcal{C}$, then X (εn)-fools every $f \in \mathcal{C}$.

(i):

Lemma: Under NW thm setup, NW-gen. is ε-nbu for all $f \in \mathcal{C}$.

Pf: Fix any $f: \{0,1\}^n \to \{0,1\}$ in $\mathcal{C}$.
Fix any $i \in [n]$, any $a \in \{0,1\}^{n-i+1}$.
Let $U \sim \mathcal{U}_s$, $X = G(U)$ (n-bit strings).

Have

$$\left| \Pr_X [f(X_1, \dots, X_{i-1}, a) = X_i] - \frac{1}{2} \right|$$

$$= \left| \mathop{\mathbb{E}}_{U_{[s]\setminus S_i}} \left[\Pr_{U_{S_i}} [f(h(U|_{S_1}), \dots h(U|_{S_{i-1}}), a) = h(U|_{S_i})] - \frac{1}{2} \right] \right|$$

$$\le \mathop{\mathbb{E}}_{U_{[s]\setminus S_i}} \left[\left| \Pr_{U_{S_i}} [f(h(U|_{S_1}), \dots h(U|_{S_{i-1}}), a) = h(U|_{S_i})] - \frac{1}{2} \right| \right]$$

For each fixing of $U_{[s]\setminus S_i}$, write $Z = U_{S_i}$.

For each $j < i$, since we fixed $U_{[s]\setminus S_i}$ & $|S_i \cap S_j| \le k$, there's a k-junta g_j s.t. $h(U|_{S_j}) = g_j(Z)$.

So

$$\left| \Pr_{U_{S_i}} [f(h(U|_{S_1}), \dots h(U|_{S_{i-1}}), a) = h(U|_{S_i})] - \frac{1}{2} \right|$$

$$= \left| \Pr_{\substack{\text{unif} \\ Z}} [f(g_1(Z), g_2(Z), \dots, g_{i-1}(Z), a) = h(Z)] - \frac{1}{2} \right|$$

$\leq \varepsilon$, b/c h is ε-hard for $C \circ \mathrm{Junta}_{r,k}$. ∎

All that remains to prove:

Lemma (ii): Let X be RV over $\{0,1\}^n$, let $f: \{0,1\}^n \to \{0,1\}$

If RV X is ε-nbu for f, then X (εn)-fools f.

Pf: "hybrid argument".

Let $B = (B_1, \ldots, B_n) \sim \mathcal{U}_n$ truly rand.

Consider hybrid dist's over $\{0,1\}^n$:

$$D_0 = (B_1, \ldots, B_n) = B$$
$$D_1 = (X_1, B_2, \ldots, B_n)$$
$$\vdots$$
$$D_{i-1} = (X_1, \ldots, X_{i-1}, B_i, \ldots B_n)$$
$$D_i = (X_1, \ldots, X_{i-1}, X_i, B_{i+1}, \ldots, B_n)$$
$$\vdots$$
$$D_n = (X_1, \ldots, X_n) = X.$$

$\triangle$ ineq: $\left| \mathbb{E}[f(X)] - \mathbb{E}[f(B)] \right| =$

$$\left| \mathbb{E}[f(D_n)] - \mathbb{E}[f(D_0)] \right|$$

$$\leq \sum_{i=1}^{n} \left| \mathbb{E}[f(D_i)] - \mathbb{E}[f(D_{i-1})] \right|. \quad (\star)$$

Fix $i \in [n]$. Have

$$\left|\mathbb{E}[f(O_i)] - \mathbb{E}[O_{i-1}]\right| = \qquad -p = (1-p) - 1$$

$$\left|\mathbb{E}[f(O_{i-1}) \mid B_i = X_i] - \left(\tfrac{1}{2}\mathbb{E}[f(O_{i-1}) \mid B_i = X_i] + \tfrac{1}{2}\mathbb{E}[f(O_{i-1}) \mid B_i \neq X_i]\right)\right|$$

$$= \left|\tfrac{1}{2}\mathbb{E}[f(O_{i-1}) \mid B_i = X_i] + \tfrac{1}{2}\mathbb{E}[\overline{f(O_{i-1})} \mid B_i \neq X_i] - \tfrac{1}{2}\right|$$

$$= \left|\mathbb{E}[f(O_{i-1}) \oplus B_i \oplus X_i] - \tfrac{1}{2}\right|$$

$$\leq \mathop{\mathbb{E}}_{B}\left[\left|\mathop{\mathbb{E}}_{X}[f(O_{i-1}) \oplus B_i \oplus X_i] - \tfrac{1}{2}\right|\right] \leq \varepsilon$$

This is $\leq \varepsilon$: for any fixing of B

if we let $g(x) = f(x_1, \ldots, x_{i-1}, B_i, \ldots B_n) \oplus B_i \oplus x_i$,

either g or $\bar{g}$ is checking whether f succ. predicts x_i given $x_1, \ldots, x_{i-1}$; so by ε-nbu of f for X, get it's $\leq \varepsilon$.

So ✡ $\leq \varepsilon n$, i.e.

X (εn)-fools f. ∎
