Last time:

- finish proof of HSL by proving "Key Fact"
- average-case l.b. for AC^0 ckts for PAR: depth-d size-$2^{cn^{1/d}}$ ckts can't achieve accuracy $> \frac{1}{2} + \frac{1}{2^{cn^{1/d}}}$
- Depth-2 avg-case lb (O'Donnell & Wimmer): depth-2 size-$2^{\frac{cn}{\log n}}$ ckts can't achieve accuracy $> 90\%$ for $ONFTRIBES(a) \wedge CNFTRIBES(b)$ (using random projections)

constant-depth circuits

- Start $\mathbb{F}_2$-polynomials: basics (every f has unique representation), saw unsolved challenge:

$x_1 x_2 \dots x_n$

Prove some $f: \{0,1\}^n \to \{0,1\}$, $f \in NP$, is $\frac{1}{n}$-hard for $OEG_{\log n}$ for some distr. $\mathcal{D}$ over $\{0,1\}^n$.

Today: Two results towards $\mathcal{D}$:

- Any degree-$(\frac{1}{4}\sqrt{n})$ ("hi deg!") $\mathbb{F}_2$-poly p has

$$\Pr_{x \sim \mathcal{D}}[\mathrm{mod}_3(x) = p(x)] \leq \tfrac{7}{8}.$$

("weak")

- Any deg-d ("low deg") $\mathbb{F}_2$-poly p has (non-trivial only if $d2^d \ll n$, i.e. $d \lesssim \log n$)

$$\Pr_{x \sim \mathcal{D}}[GIP_{d+1}(x) = p(x)] \leq \frac{1}{2} + 2^{-\Omega\left(\frac{n}{d2^d}\right)}$$

(GIP_{d+1}: generalized inner product$_{d+1}$; "strong")

- Start basic tools for derandomization / PRGs.

Scribe: Yizhi

Questions?

1st corr bd for $\mathbb{F}_2$-polys:

hi deg, weak bd on corr.

"☺" "☹"

Def $\mathrm{mod}_3(x): \{0,1\}^n \to \{0,1\}$,

$$\mathrm{mod}_3(x) = \begin{cases} 1 & \text{if } (\#1\text{'s in } x) \equiv 1 \bmod 3 \\ 0 & \text{o/w.} \end{cases}$$

$\mathrm{mod}_3(1000) = \mathrm{mod}_3(1111) = 1$

$\mathrm{mod}_3(1010) = \mathrm{mod}_3(0111) = 0.$

Thm: Any degree-$(\varepsilon\sqrt{n})$ $\mathbb{F}_2$-poly p has ($\varepsilon = \frac{1}{4}$)

"weak"

$$\Pr_{x \sim \mathcal{U}}[\mathrm{mod}_3(x) = p(x)] \le 7/8.$$

(i.e. $\mathrm{Cor}[\mathrm{mod}_3, \mathrm{DEG}_{\varepsilon\sqrt{n}}] \le \frac{3}{4}$)

$\varepsilon\sqrt{n} = d$

Hi-level idea: Fix any p, $\mathbb{F}_2$-poly of deg $d := \varepsilon\sqrt{n}$.

Define $X := \{ x \in \{0,1\}^n : p(x) = \mathrm{mod}_3(x) \}$.

Goal: $|X|$ not too big. $\left(\leq \frac{7}{8} \cdot 2^n\right)$

Intuition: mod_3 fn should have high $\mathbb{F}_2$-deg... ← means maybe mod_3 can be used to sim. high-degree $\mathbb{F}_2$-polys over $\{0,1\}^n$... ←

so maybe p can be used to sim. high-degree $\mathbb{F}_2$-polys over X... ←

but since p has low deg, (maybe) means X can't be too big...

Pf use an extension field $\mathbb{F}$ of $\mathbb{F}_2$ $(|\mathbb{F}| = 4)$.

We'll use p to represent any fn $X \to \mathbb{F}_2$ (deg d)

using an $\mathbb{F}$-poly of deg $\frac{n}{2}+d$. Means

$(\#\text{fns } X \to \mathbb{F}) = 4^{|X|} \leq (\#\mathbb{F}\text{-polys of deg } \frac{n}{2}+d)$ something

✓ (using p' s)

Setup: Assume wlog n div. by 3.

Means $\mathrm{mod}_3(1+x_1, 1+x_2, \ldots, 1+x_n) = 1$ iff

(★) $3k+1$ of the $1+x_i$'s are 1 iff

$3k+1$ " " x_i's are 0 iff

$3\ell+2$ " " x_i's are 1, i.e.

$$\sum_{i=1}^{n} x_i \equiv 2 \bmod 3.$$

Let $\mathbb{F}$ be the 4-elt. field obt. as

all polys in var t, coeff in $\mathbb{F}_2$

$$\frac{\mathbb{F}_2[t]}{t^2+t+1}$$ "modding out" by t^2+t+1

i.e. $\mathbb{F} = \{0, 1, t, 1+t\}$.

Do math as usual with (mod 2), but using identity $t^2+t+1=0$. i.e. $t^2 = -t-1 = t+1$.
$t^2+t=1$

Ex: $t^3 = ?$ $\quad t^3 = t\cdot(t^2) = t(t+1) = t^2+t = 1.$

Define $h: \{1, t\} \to \mathbb{F}_2$ be "change of domain" (affine) map

$$h(\alpha) = \frac{\alpha+1}{t+1} = t(\alpha+1) = t\alpha + t$$

$h(1) = 0$
$h(t) = t^2+t = 1$

$h(1) = 0$
$h(t) = 1$

Claim: For any $y \in \{1,t\}^n$, have

$t^{\text{something}}$ 0 or 1 0 or 1

$$y_1 y_2 \cdots y_n = 1 + (t+1)\cdot \mathrm{mod}_3(h(y_1), \ldots h(y_n)) + (t^2+1)\,\mathrm{mod}_3(1+h(y_1), \ldots, 1+h(y_n))$$

i.e. (# t's in y)

Pf: $\mathrm{mod}_3(h(y_1), \ldots, h(y_3)) = \begin{cases} 1 & \text{iff } \sum h(y_i) \equiv 1 \bmod 3 \\ 0 & \text{o/w} \end{cases}$

And by $\star$, $\mathrm{mod}_3(1+h(y_1), \ldots, 1+h(y_n)) = \begin{cases} 1 & \text{iff \# t's in y is } \equiv 2 \bmod 3 \\ 0 & \text{o/w.} \end{cases}$

#t's in y: 0, 1 or 2 mod 3.

0 mod 3: (b/c $t^3=1$)
$LHS = t^{3k} = 1$, $RHS = 1 + 0 + 0$ ✓

1 mod 3:
$LHS = t^{3k+1} = t$, $RHS = 1 + (t+1) + 0 = t$ ✓

2 mod 3:
$LHS = t^{3k+2} = t^2$, $RHS = 1 + 0 + (t^2+1) = t^2$ ✓

■

Pf of thm:

Fix p to be any poly $\{0,1\}^n \to \{0,1\}$ of deg d. ($\mathbb{F}_2$-poly)

Let $\delta = \Pr_{u \sim \mathbb{F}_2^n}[p(u) \neq \mathrm{mod}_3(u)]$.

Goal: $\delta \geq 1/8$.

Let $p' : \{1,t\}^n \to \mathbb{F}$ be (y_i's are vars)

$$p'(y_1,\dots,y_n) := 1 + (t+1)\,p(h(y_1),\dots h(y_n)) + (t^2+1)\,p(1+h(y_1),\dots,1+h(y_n)).$$

Obs: if p exact same as mod_3, then p' would be exactly $y_1 \cdots y_n$ (using Claim)

Have $\Pr_{y \sim \{1,t\}^n}[p'(y_1,\dots,y_n) = y_1 \cdots y_n] \geq 1 - 2\delta$ (using Claim)

(b/c both $(h(y_1),\dots,h(y_n))$ & $(1+h(y_1),\dots,1+h(y_n))$ are unif. over $\{0,1\}^n$ when $y \sim \{1,t\}^n$.)

Since $\deg(h) = 1$, $\deg(p) = d$, have $\deg(p') \leq d$.

Define $S \subseteq \{1,t\}^n$ to be

$$S = \{ y \in \{1,t\}^n : y_1 \cdots y_n = p'(y_1,\ldots,y_n) \}.$$

Just showed $|S| \geq 2^n(1-2\delta)$.

Consider any $f: S \to \mathbb{F}$.

Can write f as multilin. poly: ✓

$$f(y_1,\ldots,y_n) = \sum_{(a_1,\ldots,a_n)\in\{1,t\}^n} f(a_1,\ldots,a_n) \prod_{i=1}^{n} (1 + h(y_i) + h(a_i)).$$

$y_i = a_i$: $1 + 2h(a_i) = 1$

$y_i \neq a_i$: $1 + 1 + 0 = 0$

1 if $y_i = a_i$ $\forall i$

0 o/w

Key claim: Any multilin. monom. M (over $y_1,\ldots,y_n$) of ($|M| > \frac{n}{2}$) deg $> \frac{n}{2}$ can be replaced by a poly of deg $\leq \frac{n}{2} + d$, without affecting value on any string in S:

$$\prod_{i\in M} y_i = \underbrace{y_1 \cdots y_n}_{y_i} \cdot \prod_{i\notin M} (y_i t + y_i + t) \overset{\text{b/c considering } y\in S}{=} \underbrace{p'(y_1,\ldots,y_n)}_{\text{deg } d} \cdot \prod_{i\notin M} (y_i t + y_i + t)$$

deg $\leq \frac{n}{2}$.

$i \in M$: y_i on LHS, $+$ on RHS

$i \notin M$: no y_i on LHS

RHS: $y_i \cdot (y_i t + y_i + t)$

$y_i = 1$: $1 \cdot (1 + t + t) = 1$

$y_i = t$: $t \cdot (t^2 + 2t) = t^3 = 1$

Do this for every monom. in poly for f,

+ write $f: S \to \mathbb{F}$ as a poly over $\mathbb{F}$ of deg $\le \frac{n}{2}+d$.

Since $|\mathbb{F}|=4$, there are $4^{|S|}$ fns $f: S \to \mathbb{F}$,

+ there are $|\mathbb{F}|^{\sum_{i=0}^{\frac{n}{2}+d}\binom{n}{i}}$ ($=4$) multilin. polys over $\mathbb{F}$ of deg $\le \frac{n}{2}+d$. So

$$2^n(1-2\delta) \le |S| \le \sum_{i=0}^{\frac{n}{2}+d}\binom{n}{i} \le 2^{n-1} + d\cdot\binom{n}{n/2}$$ (recall $d=\varepsilon\sqrt{n}$)

$$\le 2^n\left(\frac{1}{2} + \frac{d}{\sqrt{n}}\right)$$

$$= 2^n\left(\frac{1}{2}+\varepsilon\right)$$

So $1-2\delta \le \frac{1}{2}+\varepsilon$, i.e.

$\delta \ge \frac{1}{4} - \frac{\varepsilon}{2}$. So $\varepsilon = \frac{1}{4} \Rightarrow \delta \ge \frac{1}{8}$.

Break

Now:

- Any deg-d ("low deg") $\mathbb{F}_2$-poly p has (non-trivial only if $d2^d << n$, i.e. $d \lesssim \log n$)

$$\Pr_{x\sim\mathcal{U}}\left[GIP_{d+1}(x) = p(x)\right] \le \frac{1}{2} + 2^{-\Omega\left(\frac{n}{d2^d}\right)}$$

(GIP_{d+1}: generalized inner product$_{d+1}$; "strong")

Can show: $IP(x) = x_1 x_2 + \cdots + x_{n-1} x_n$ (over $\mathbb{F}_2$)

has very low corr. w/ any deg-1 $\mathbb{F}_2$-poly:

$(+1)$ $x_1 + x_3 + x_4 + x_7$

$\deg(p) = 1 \Rightarrow \Pr_u[IP(u) = p(u)] = \frac{1}{2} \pm \frac{1}{2^{n/2}}$.

What's hard for deg 2?

→ maybe $x_1 x_2 x_3 + x_4 x_5 x_6 + \cdots$?

Define $GIP_{d+1}(x) = x_1 \cdots x_{d+1} + x_{d+2} \cdots x_{2d+2} + \cdots$

$\cdots + x_{n-d} x_{n-d+1} \cdots x_n$.

Setup: Given $f: \mathbb{F}_2^n \to \{0,1\}$,

write $e(f) := (-1)^f$, so $e(0) = 1$

$e(1) = -1$.

Write $F(x)$ to mean $e(f(x))$.

F	± 1
f	$0/1$

$F, G \to \{\pm 1\}$: $Cor[F, G] = |\mathbb{E}[F \cdot G]|$

Goal: analyze $Cor[F, Deg_d]$. ?

Would like to relate ↓ to $\mathrm{Cor}[\text{something}, \mathrm{Deg}_{d-1}]$

Squaring $\mathrm{Cor}[\,,\,]$: useful!

(Everything always indep. unif. over $\mathbb{F}_2^n$)

Let's explore...

Fix any $F : \mathbb{F}_2^n \to \{\pm 1\}$, $(F = e(f))$

Fix any deg-d $P : \mathbb{F}_2^n \to \{0,1\}$, $P = e(P)$.

$$\mathrm{Cor}[F,P] = \left| \mathop{\mathbb{E}}_x [F(x)(-1)^{P(x)}] \right|.$$

Square it:

$$\mathrm{Cor}[F,P]^2 = \mathop{\mathbb{E}}_x [F(x)(-1)^{P(x)}]^2$$

(!)

$$= \mathop{\mathbb{E}}_x [F(x)(-1)^{P(x)}] \cdot \mathop{\mathbb{E}}_y [F(y)(-1)^{P(y)}]$$

$$= \mathop{\mathbb{E}}_{x,y} [F(x)F(y)(-1)^{P(x)}(-1)^{P(y)}].$$ $(y = x+h)$ This is

$$\mathop{\mathbb{E}}_h \left[\mathop{\mathbb{E}}_x [F(x)F(x+h)(-1)^{P(x)}(-1)^{P(x+h)}] \right].$$

$$(-1)^{P(x)}(-1)^{P(x+h)} = e(P(x)) \cdot e(P(x+h))$$

$$= e(P(x) + P(x+h))$$

Key Obs: For any fixed h, for P a deg-d $\mathbb{F}_2$ poly,

$p(x) + p(x+h)$ is a deg-$(d-1)$ poly!

e.g. $p = x_1 \cdots x_d$: $p(x) + p(x+h) =$

$x_1 \cdots x_d + (x_1+h_1)\cdots(x_d+h_d)$

$x_1 \cdots x_d$ + lower deg stuff

So (!) = $\mathop{\text{Avg}}_h$ of Cor of (something) $\leq F(x)F(x+h)$

with a deg-$(d-1)$ poly.

Made progress! :)

Notation: write $F^{+y}(x)$ for $F(x+y)$

Def: (Gowers uniformity)
Let $F : \mathbb{F}_2^n \to [-1,1]$, let $k \geq 0$ integer.
The *k-uniformity of f* is

$$U_k(F) = \mathop{\mathbb{E}}_{h_1,\ldots h_k, x} \left[\prod_{S \subseteq [k]} F^{+\sum_{j \in S} h_j}(x) \right].$$

Interpret.: any fixed $h_1, \ldots, h_k$ define a k-dim "cube" of shifts; prod. of F across all of pts in cube, avg of

---

Ex: $k=0$: $U_0(F) = \mathbb{E}[F]$. $y = x+h_1$

$k=1$: $U_1(F) = \mathop{\mathbb{E}}_{h_1,x}[F(x)F^{+h_1}(x)] = \mathop{\mathbb{E}}_{x,y}[F(x)F(y)]$

$= \mathop{\mathbb{E}}_{x}[F(x)]^2 \geq 0$

$$= \mathop{\mathbb{E}}_{h_1}\left[U_0\left[F\cdot F^{+h_1}\right]\right]$$

$$k=2:\ \mathop{\mathbb{E}}_{h_1,h_2,x}\left[F(x)F^{+h_1}(x)F^{+h_2}(x)F^{+h_1+h_2}(x)\right]$$

$$= \mathop{\mathbb{E}}_{h_2}\left[U_1\left[F\cdot F^{+h_2}\right]\right] \geq 0.$$

In general $$U_{k+1}[F] = \mathop{\mathbb{E}}_{h_{k+1}}\left[U_k\left[F\cdot F^{+h_{k+1}}\right]\right] \geq 0.$$

Example (useful!):

Lemma: ($(d+1)$-unif. of AND)

Let $F = e(f)$, $f = x_1,\dots x_{d+1}$ $\quad f: \mathbb{F}_2^{d+1} \to \{0,1\}$

$F: \mathbb{F}_2^{d+1}$

so $F(1^{d+1}) = -1$

$F(\text{anything else}) = 1.$

Then $U_{d+1}(F) \approx 0.6$.

$$U_k(F) = \mathop{\mathbb{E}}_{h_1,\dots h_k,x}\left[\prod_{S\subseteq[k]} F^{+\sum_{j\in S} h_j}(x)\right].$$

Pf: $U_{d+1} = 1-2p$, where

$$p = \Pr\left[\prod_{S\subseteq[d+1]} F^{+\sum_{j\in S} h_j}(x) = -1\right]$$

If $h_1 = e_1 = (100\dots0)$
$\vdots$
$h_{d+1} = e_{d+1} = (0\dots01)$: $\sum_{j\in S} h_j$ varies over $\mathbb{F}_2^{d+1}$, $\forall$

$\prod_{S\subseteq[d+1]} F^{+\sum_{j\in S} h_j}(x)$ is

prod. of $F(z)$ as z varies over all of $\mathbb{F}_2^{d+1}$, (in fact, true for $h_1, \dots, h_{d+1}$ any basis). F is -1 once, so $\prod_{\text{all } z \in \mathbb{F}_2^{d+1}} F(z) = -1$.

OTOH, if $h_1, \dots, h_{d+1}$ not a basis, then for any x, the arguments to $F^{+\sum_{j \in S} h_j}(x)$ each occur an even # times, $\forall$

$\prod_{S \subseteq [d+1]} F^{+\sum_{j \in S} h_j}(x)$ is $+1$.

So $p = \Pr_{h_1, \dots, h_{d+1}}[h_1, \dots, h_{d+1} \text{ basis of } \mathbb{F}_2^{d+1}]$

$$= \left(1 - \frac{1}{2^{d+1}}\right) \cdot \left(1 - \frac{2}{2^{d+1}}\right) \cdot \left(1 - \frac{4}{2^{d+1}}\right) \cdots \left(1 - \frac{2^d}{2^{d+1}}\right)$$

$$= \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{7}{8} \cdot \frac{15}{16} \cdot \cdots \cdot \left(1 - \frac{1}{2^{d+1}}\right) \approx 0.2.$$

(A) Lemma: Let $F: \mathbb{F}_2^n \to \{\pm 1\}$ any fn, let $P = e(p)$, p a deg-d $\mathbb{F}_2$-poly. Have $\mathrm{Cor}[F, P] \le U_{d+1}(F)^{\frac{1}{2^{d+1}}}$.

Fact (immediate from def) (B)

Let $F_1, F_2 : \mathbb{F}_2^n \to \{\pm 1\}$. Define

$$G(x,y) = F_1(x) \cdot F_2(y).$$

Then $U_k(G) = U_k(F_1) \cdot U_k(F_2)$.

Thm: Let $GIP_{m,d+1}$ be the deg-$(d+1)$ poly over $\mathbb{F}_2^n$, $n = m(d+1)$

$$GIP_{m,d+1} = \overbrace{x_1 \cdots x_{d+1} + \cdots + x_{n-d} \cdots x_n}^{m \text{ monom's.}}$$

Then $Cor\{ {}_e GIP_{m,d+1} \, {}_e DEG_d \} \le \exp\left(-\Omega\left(\frac{n}{d \cdot 2^d}\right)\right)$

Pf: $\le U_{d+1}({}_e GIP_{m,d+1})^{\frac{1}{2^{d+1}}}$ (A)

$$= U_{d+1}(e(ANO_{d+1}))^{\frac{m}{2^{d+1}}}$$

$$\le (0.6)^{\frac{m}{2^{d+1}}} \qquad m = \frac{n}{d+1}$$ ▨

Next time: PRG tools! (after lemma)