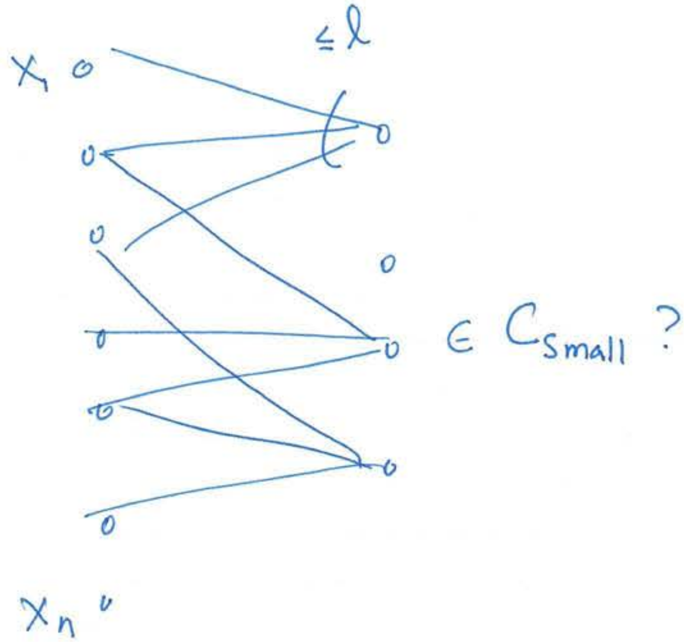
CS229r - LECTURE 21

4/11/17

TODAY
- Testing Tensor Product Codes
- Testing Low Degree Polynomials

Recall:

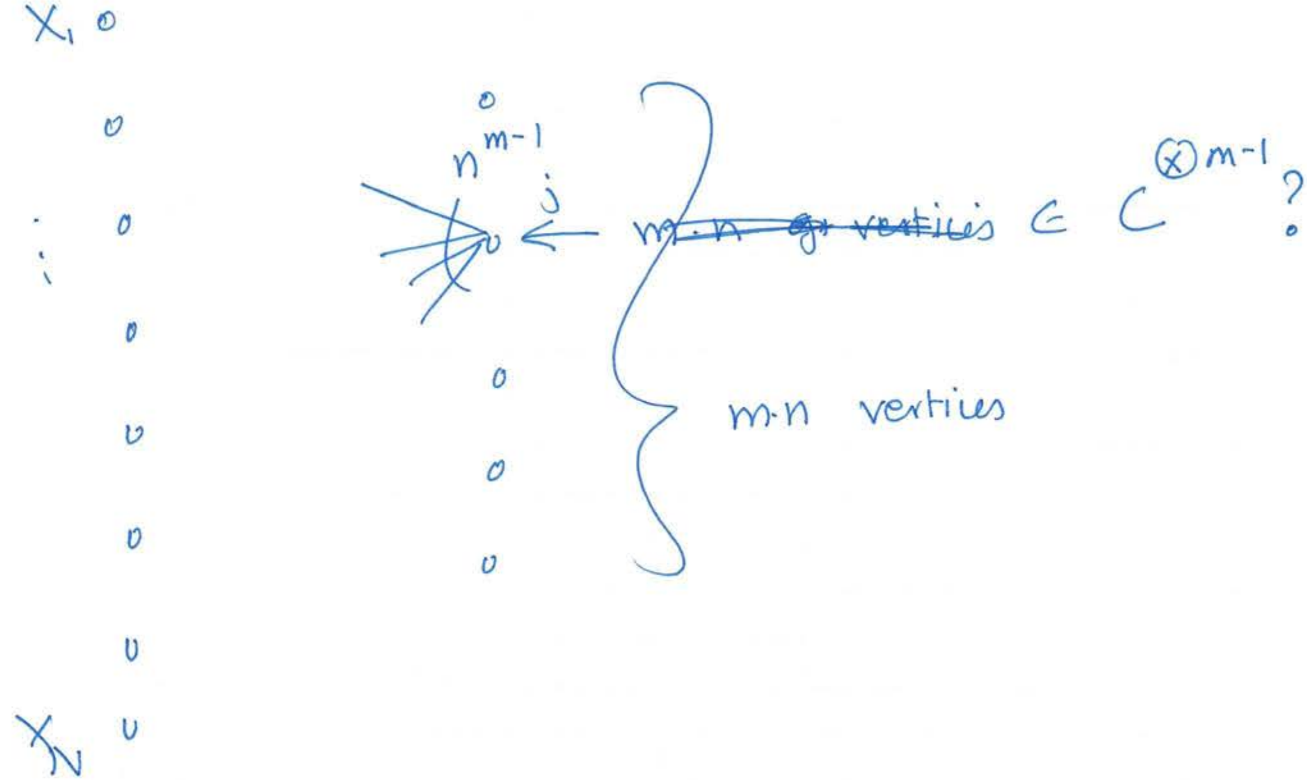
LDPC view of LTC:



- $C_{big} = \{ (x_1 .. x_n) \mid \forall j \in R \quad x|_{\Gamma(j)} \in C_{small} \}$
- Test: Pick random right vertex j & verify $x|_{\Gamma(j)} \in C_{small}$
- ϵ-Soundness: $\Pr_j[\text{reject } x] \geq \epsilon \cdot \delta(x, C_{big})$
- α-Robustness: $\mathbb{E}_j\left[\delta(x|_{\Gamma(j)}, C_{small}) \right] \geq \alpha \cdot \delta(x, C_{big})$

Test α-Robust $\Rightarrow$ Test α-sound. $\Rightarrow$ Test $\frac{\alpha}{\ell}$-robust.

$\underline{C^{\otimes m}}$



$N = n^m$

<u>Viderman Thm</u>: $\forall\, m \geq 3,\ \delta > 0\ \exists\, \alpha > 0$ s.t. $\forall\, C \quad \delta(C) \geq \delta$

C^{m-1} test ~~is~~ for C^m is α-robust.

<u>Proof</u>: will do $m=3$ for simplicity. Idea works $\forall\, m \geq 3$.

Given: $f : [n]^3 \to \mathbb{F}_q$ ~~want to~~

Let $A, B, D : [n]^3 \to \mathbb{F}_q$ be s.t.

(1) $\forall\, i \quad A(i,\cdot,\cdot),\ B(\cdot,i,\cdot),\ D(\cdot,\cdot,i) \in C \otimes C$

(2) $\dfrac{\delta(f,A) + \delta(f,B) + \delta(f,D)}{3}$ = local dist. of f from $C \otimes C$ test $\triangleq \tau$

<u>Define</u> (i,j,k) to be <u>Good-point</u> if

$$A(i,j,k) = B(i,j,k) = D(i,j,k)$$

Bad-point otherwise.

<u>Define</u> $(i,\cdot,\cdot)$ etc. to be <u>Bad-plane</u> if

more than $\frac{\delta^2 \cdot n^2}{2}$ ~~points on~~ pairs (j,k) make (i,j,k) <u>Bad</u>

<u>Claim</u>: Bad-points live on Bad-Planes.

<u>Proof</u>: Suppose $A(i,j,k) \neq B(i,j,k)$

$\Rightarrow A(i,j,\cdot) \neq B(i,j,\cdot)$

$\Rightarrow \delta(A(i,j,\cdot), B(i,j,\cdot)) \geq \delta$ [since both are codewords of C]

$\Rightarrow$ for every k' s.t.

$A(i,j,k') \neq B(i,j,k')$ we have

either $A(i,j,k') \neq D(i,j,k')$ or

$B(i,j,k') \neq D(i,j,k')$ ← say this happens more than for $\frac{\delta n}{2}$ k's.

then $A(i,\cdot,k') \neq D(i,\cdot,k')$ for $\frac{\delta n}{2}$ k's.

so $A(i,j',k') \neq D(i,j',k')$ for $\frac{\delta n}{2} \cdot \delta n$ (j',k')

$\Rightarrow$ A is Bad.

☒

Throw away i if $A(i,\cdot,\cdot)$ bad
j $B(\cdot,j,\cdot)$ bad
k $D(\cdot,\cdot,k)$ bad

~~Remaining~~ Say (i,j,k) excellent if $A(i,\cdot\cdot)$ good
$B(\cdot,j,\cdot)$ good
$D(\cdot\cdot k)$ good

Claim 1: ~~#~~ excellent points form $(1-\delta)n \times (1-\delta)n \times (1-\delta)n$ cube. (*)

$\Downarrow$

Claim 2: if (*) then A, B, D can be extended uniquely from excellent set ~~of~~ to whole cube. $[n]\times[n]\times[n]$ to get el't of $C\otimes C\otimes C$.

Claim 3: Extended function close to original function.

Proof of Claim 1: ~~Pr[test rejects | bad point] $\geq \frac{1}{3}$~~

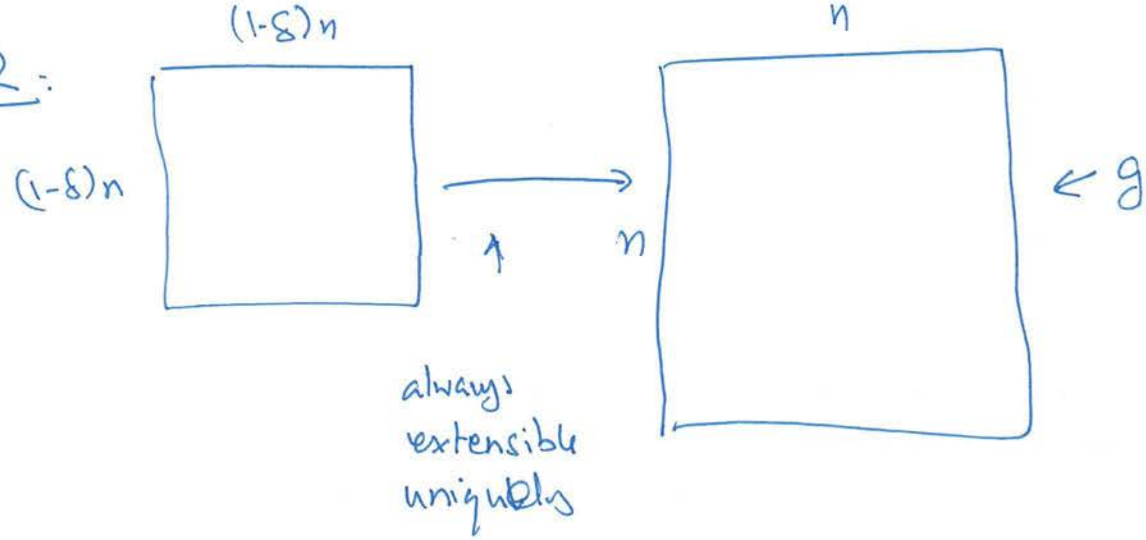
~~$\Rightarrow$ # bad points $\leq$~~

Bad plane $A(i,\cdot,\cdot)$ has $\frac{\delta^2}{2}$ fraction bad points.

$\Rightarrow$ fraction bad i planes $\leq \frac{3T}{\delta^2/2} \leq \frac{6T}{\delta^2} < \delta$ [will arrange]

$\left[T < \frac{\delta^3}{6}\right]$.

Claim 2:



Proof: follows from tensor product + erasure decoding. ☒

Proof of Claim 3:

Fraction of pts on Bad planes $\leq \frac{18 \cdot \tau}{\delta^2}$

if $f \neq g \in C \otimes C \otimes C$ then pt is on bad plane

Or $f(i,j,k) \neq (A(i,j,k) = B(i,j,k) = C(i,j,k))$

Fraction of such pts $\leq \tau$.

$\Rightarrow \text{dist}(f,g) \leq \tau + \frac{18\tau}{\delta^2} = \left(1 + \frac{18}{\delta^2}\right)\tau.$

$\Rightarrow$ Test is $\left(1 + \frac{18}{\delta^2}\right)$-robust — in general some dependence on m.

Low degree Testing [RS, ALMSS, ... GHS]

- $RM(m,d,q)$: m-var. poly over $\mathbb{F}_q$ of deg $\leq d$.
- Test : Pick random 2-dim plane P ;
  verify $\deg(f|_P) \leq d$.
- Robustness :

$$\rho(f) \triangleq \mathop{\mathbb{E}}_{P}\left[\delta\left(f|_P, \mathbb{F}_q^{\leq d}[t_1,t_2]\right)\right]$$

$$\delta(f) \triangleq \delta(f, \mathbb{F}_q^{\leq d}[x_1 \ldots x_m])$$

Thm: $\forall\, \delta > 0\ \exists\, \alpha > 0$ s.t. $\forall\, m, q, d$ s.t. $1 - \frac{d}{q} \geq \delta$

the two-dim test is α-robust

Lemma 1: Suffices to prove theorem for $m \leq 5$.

Lemma 2: Thm hold for $m \leq 5$.

Proof Ideas for Lemmas 2 & 1

Lemma 2:

(1) Say direction P is good if Planes of form $\{a+P\}$ are close to deg. d poly for most a.

- Say $m=3$
- Suppose XY-plane, XZ-plane & YZ-plane are good for f
- Then by Viderman; f is close to some polynomial g with $\deg_x g, \deg_y g, \deg_z g \leq d$
- if $d \leq \frac{q}{3}(1-\epsilon)$ then $\deg g < (1-\epsilon) q$.
- So whp. g on random plane will be close f, But whp g on random plane has $\deg g = \deg(g)$

$\Rightarrow$ while f on random plane is close to deg d poly

$\Rightarrow$ g has deg d. ☒

$d > \frac{q}{3}$ non-trivial (omitted) : Actually $d \geq \frac{q}{2}$ not true!

$\frac{q}{2} > d \geq \frac{q}{3}$: Non-trivial

Lemma 1: [Ideas going back to Blum Luby Rubinfeld, R + S]

- Key notion: Let g = Local-decoder (f).
- Need to prove ① g close to f.

② g is a deg. d poly.

① Easy: if $g \neq f$ at x, then pr[test through x rejects]

$\geq \frac{1}{2}$.

[Markov $\Rightarrow$ $\Pr[f(x) \neq g(x)] \leq 2 \cdot T(f)$.]

② g is deg d?

Fix x; $\text{Decoder}^f(\ell_1; x)$ = Decode $f|_{\ell_1}$ & output value at x.

- Question: is $\forall x$ $\Pr_{\ell_1,\ell_2}[\text{Decoder}^f(\ell_1,x) = \text{Decoder}^f(\ell_2,x)]$?

(Necessary, and morally also sufficient)

- Answer: Yes ... for following reason.

Pick ℓ_1, ℓ_2 randomly through x & then a random 3-dim cube C containing ℓ_1, ℓ_2.

Typical 2-plane P in C is random; ⇒ $f|_P$ close to deg d poly.

By lemma 2 ⇒ $f|_C$ close to deg d poly. g

⇒ ~~$f|_{l_1}$ close to~~ Nearest poly to $f|_{l_1} = g|_{l_1}$

& Nearest poly $f|_{l_2} = g|_{l_2}$

⇒ $\text{Decoder}^f(l_1; x) = \text{Decoder}^f(l_2; x) = g(x)$.

Can use this to prove $g|_l$ is a deg d poly $\forall l$.

$$\left[\forall x, \forall l \ni x \quad g(x) = \text{Decoder}^g(l; x) \right]$$

⇓

$\deg(g) \leq d$ if $d < q/2$.

Asides on LTCs

Major Ingredients in PCP theory;

Tests of Long Code;
Short Long Code;
Hadamard Code;
Low-degree Polynomials

} All central.