CS229r - LECTURE 20

4/6/17

TODAY: 1) Finish High Rate LDCs

2) LTC constructions.

2.1) Redundant LDPCs

2.2) Tensor Codes & Testing $\Rightarrow$ RM-like perf.

2.3) Zig-Zag Codes & Testing. $\Rightarrow$ ~ polylog locality

---

- LDC: See notes for Lecture 19

Terminology: LDPC codes: Low Density Parity Check

= Gallager codes

= Tanner codes

= Sipser-Spielman Codes.

Low Density: Parity Check Matrix = Sparse

$\Leftrightarrow$ Underlying graph sparse

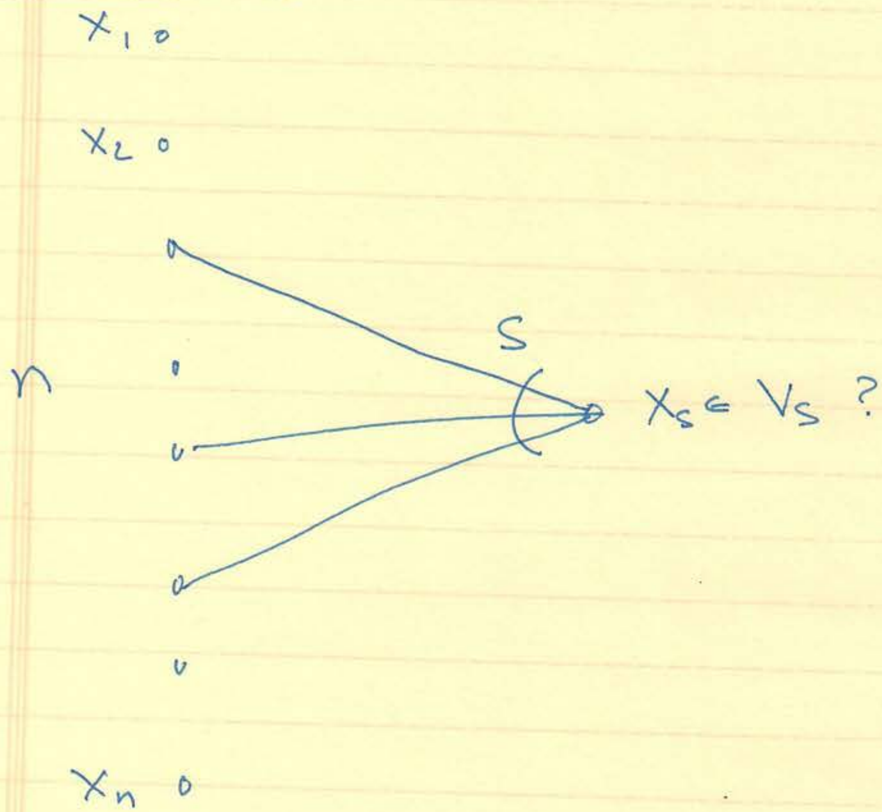
$\Leftrightarrow$ average constant degree.

Contrast: LDPC & LTCs

LTC: Picks randomly $S \subseteq [n]$; $|S| \le \ell$

& verify $x|_S \in V_S \subseteq \mathbb{F}_2^{|S|}$

(i) LTC $\Rightarrow$ LDPC



"Strong soundness" $\Rightarrow$ $\forall S$ $x_S \in V_S \iff x \in C$

~~$\delta(x,C)$~~

$\Pr[x_S \notin V_S] \ge \epsilon \cdot \delta(x,C)$.

$= 0 \Rightarrow \delta(x,C) = 0 \Rightarrow x \in C$.

(ii) But LDPC $\not\Rightarrow$ LTC [BenSasson Harsha Raskhodnikova]

– Key Issue: Need redundant local constraints.

i.e. Removing ~~1/2~~ one or few or ~~constant fraction of constraints~~ $\frac{1}{R}$ fraction of constraints should not change the code.

– How can we get redundancy.

∘ Ans 1: By building code with many symmetries.

E.g. RM codes have constraint for each line.

$$\# \text{ coordinates} = n = q^m$$
$$\# \text{ constraints} = \binom{q^m}{2} \approx n^2 \gg n.$$

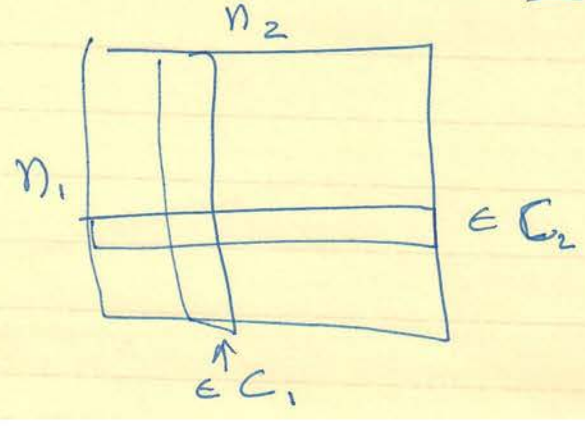
∘ Ans 2: Tensor Products [Ben-Sasson-Sudan]

<u>Tensor Product Code</u>

$C_1 = [n_1, k_1, d_1]_q$ & $C_2 = [n_2, k_2, d_2]_q$

$C_1 \otimes C_2 = [n_1 n_2, k_1 k_2, d_1 d_2]_q$ code with codewords

=

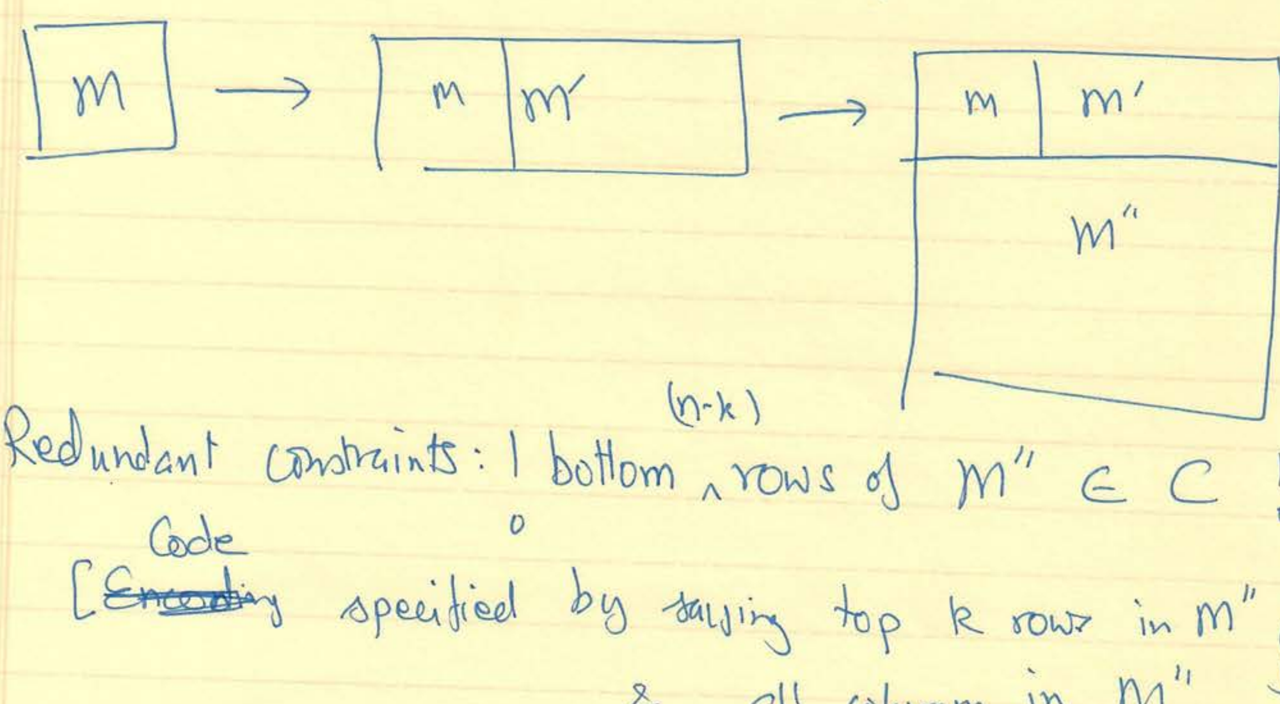


with every column in C_1
every row in C_2.

$\boxed{\text{Exercise: Prove dimension \& distance}}$.

<u>Redundancy in Tensor Product Codes</u> Let $C_1 = C_2 = C$.

- Code has length n^2
- But specified by $2n$ constraints; assume C is a systematic code with first k coordinates being message.
- Then given $k \times k$ matrix M, its encoding may be obtained by expanding rows into codewords of C [giving matrix $M' \in \mathbb{F}^{k \times n}$] & then expanding columns into codewords of C giving $n \times n$ matrix M''.



- Redundant constraints: bottom $(n-k)$ rows of $M'' \in C$!

[~~Encoding~~ Code specified by saying top k rows in M'' & all columns in M'' $\Big\} \in C$]

Basic Testing Question

if $\Pr[\text{random row} \in C] \geq$ ~~.9~~ $1-\epsilon$

& $\Pr[\text{random colum} \in C] \geq 1-\epsilon$

then $\delta(M, C\otimes C) \leq 1-\epsilon''$?

Robust Testing Question

if $\frac{1}{2}\left[\mathbb{E}_{row}\left[\delta(M|_{row}, C)\right) + \mathbb{E}_{column}\left[\delta(M|_{colum}, C)\right)\right] \leq \beta$

$\Rightarrow \delta(M, C\otimes C) \leq \alpha \cdot \beta.$

Why Robustness? $\boxed{\text{if } C\otimes C\text{-test is } \alpha\text{-robust} \text{ \& } C \text{ is } (\epsilon, \ell)\text{-locally testable, then } C\otimes C \text{ is } \left(\frac{\epsilon}{\alpha}, \ell\right)\text{-locally testable.}}$

↑ Proposition ↑

Hope: $\forall\, \delta\ \exists\, \alpha$ s.t. if C is a code of dist $\geq \delta$
[BSS] then ~~$C\otimes C$ is α~~
C-test for $C\otimes C$ is α-robust.

Example [Paul Valiant]: No.

Generalizing: $C^{\otimes m} = C \otimes C \otimes \dots C$

$C^{\otimes l}$ test of $C^{\otimes m}$: Pick random l-dim axis parallel surface. S
Verify $\delta(M|_S, C^{\otimes l}) \le$ small.

Theorem [Ben-Sasson, S.., Viderman]
$\forall m \geq 3 \; \forall \delta \; \exists \alpha$ s.t. if $\delta(C) \geq \delta$ then
$C^{\otimes m-1}$ test for $C^{\otimes m}$ is α-robust.

Corollary
$\forall m \geq 3 \; \forall \delta \; \exists \alpha'$ s.t. if $\delta(C) \geq \delta$ then
$C^{\otimes 2}$ test for $C^{\otimes m}$ is α-robust.

Proposition: A-test for B is α_1 robust
& B-test for C is α_2-robust
$\Rightarrow$ A-test for C is $(\alpha_1 \alpha_2)$-robust.

Using Tensor Codes directly

Thm [Viderman]: $\forall \alpha, \beta > 0 \ \exists \delta$ s.t. for large $N \ \exists$ codes of length N, Rate $\geq 1-\alpha$, locality $\leq N^{\beta}$, distance $\geq \delta$

$\boxed{\text{Proof: Exercise}}$ (analogous to Kopparty, Saraf, Yekhanin).

~~Can do~~
But dependence of δ on α, β much worse $\left(\delta = (\alpha\beta)^{1/\beta}\right)$

Tensor Codes + Distance-Amplification

Thm [KMRS1]: $\exists \, n^{o(1)}$ function $\ell(n)$ s.t. $\forall \, \delta \ \exists$ codes of rate $1-\delta-o(1)$ & dist δ that are $\ell(n)$-locally testable.

← barely subpolynomial; worse than for LDCs.

But: Can do much better:

We have two operations:

- Tensor Product: Makes Code longer;
  Preserves locality;
  Makes distance worse;
  Makes Rate worse
- A-L Transform: Code longer;
  Loses locality;
  Improves distance;
  Makes rate worse.

Idea: Will pick $\delta_0 = o(1)$

m - repetitions of Tensor Product followed by A-L Transform

Rate	R	$\rightsquigarrow$	R^2	$\rightsquigarrow$	$R^2 - \delta_0$
dist	δ_0	$\rightsquigarrow$	δ_0^2	$\rightsquigarrow$	δ_0
locality	ℓ	$\rightsquigarrow$	ℓ	$\rightsquigarrow$	ℓ/δ_0
length	n_i	$\rightsquigarrow$	n_i^2	$\rightsquigarrow$	$n_i^2 = n_{i+1}$

~~After~~ Start with $n_0 = \underbrace{\text{near const.}}_{\text{poly}(1/\delta_0)}$; $R = 1 - \delta_0$

$$n_i = n_0^{2^i} \; ; \; R_i = R - 2^i \delta_0 \; ; \; \ell_i = \ell / \delta_0^i$$

Yields codes of length N with $R = 1 - o(1)$; $\ell_i = (\log N)^{\log N}$.

(Need some care)

Tensor products testable only by $\square$'s ..... But can work this out. Details omitted.

Concluding:

LTCs $\rightsquigarrow$ very strong performance

LDCs $\rightsquigarrow$ weaker but substantially $o(n)$ for no-cost!

LRCs $\rightsquigarrow$ \$\$\$

Other concepts

Relaxed LDCs: Either recover a bit or say "there are too many errors".

Usually as good as LTCs...