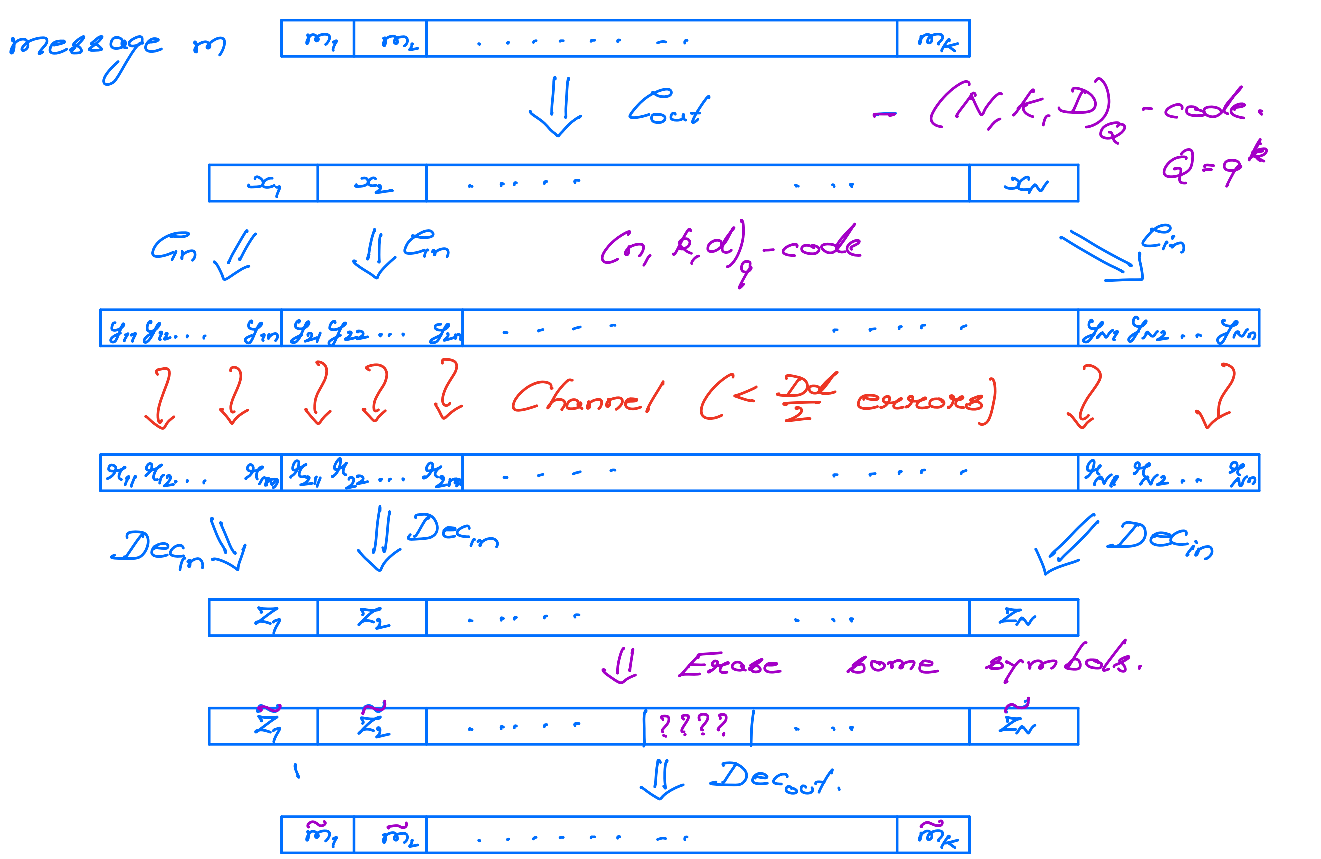
Today

- Forney's GMD Decoding
- Expander Codes.

CS5.318.1
Coding Theory
Lecture 12 (2022-10-10)
Instructor: Prahladh Harsha.

Decoding Concatenated Codes

$C_{comp} = (Nn, Kk, Dd)_q$-code



Qn: If #errors $< Dd/2$, then $\tilde{m} = m$?

Forney's requirements for GMD decoding (Generalized minimum distance)

C_{out} – $(N, K, D)_Q$ -code.

(Eff) Decoder Dec_{out} which can decode from

E errors + S erasures provided $2E + S < D$.

(eg: Reed Solomon code w/ WB decoder).

C_{in} :– $(n, k, d)_q$ - code.

Decoder Dec_{in} which can handle e errors provided $2e < d$.

GMD Decoder:

Input: $(x_1, \ldots x_N) \in [q^n]^N$ where each $x_i = (x_{i1}, \ldots x_{in}) \in [q]^n$

Inner Phase:

For each $i \in [N]$

(i) Run Dec_{in} on $x_i = (x_{i1} \ldots, x_{in})$ to obtain $z_i = (z_{i1} \ldots z_{ik}) \in [Q] \cong [q]^k$

(ii) $e_i = \min\{\Delta(C_{in}(z_i), x_i), d/2\}$

Outer Phase

For each $i \in [N]$

(i) $\tilde{z}_i \leftarrow \begin{cases} \text{"?"} & \text{w/ prob } e_i/(d/2) \\ z_i & \text{otherwise} \end{cases}$

Run Dec_{out} on $(\tilde{z}_1, \tilde{z}_2, \ldots, \tilde{z}_N)$ to obtain $(\tilde{m}_1, \ldots, \tilde{m}_k) \in [Q]^k$.

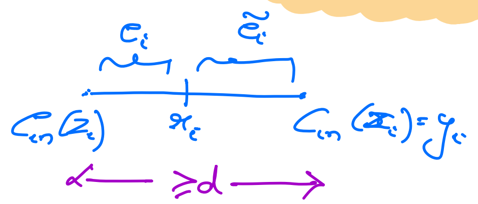
Analysis (show in expectation, that the above algorithm decodes correctly provided $\#\text{errors} < Dd/2$)

$\tilde{e}_i := \#$ errors in i^{th} block $\quad / \sum_{i \in [N]} \tilde{e}_i = \#\text{errors}$

$e_i = \min\{\Delta(C_{in}(z_i), x_i), d/2\}$.

If $z_i = x_i$ $\quad \Rightarrow \quad e_i = \tilde{e}_i < d/2$.
$(C_{in}(z_i) = y_i)$

If $z_i \neq x_i$ $\quad \Rightarrow \quad \tilde{e}_i \geq d - e_i$



For $i \in [N]$

$U_i = \begin{cases} 1 & \text{if } i^{th} \text{ block is erased} \\ 0 & \text{otherwise} \end{cases}$

$V_i = \begin{cases} 1 & \text{if } i^{th} \text{ block is not erased} \wedge x_i \neq z_i \\ 0 & \text{otherwise} \end{cases}$

Suff if we show $\sum_{i \in [N]} \mathbb{E}[U_i + 2V_i] < D$

Focus on specific $i \in [N]$.

Claim: $\mathbb{E}[U_i + 2V_i] < \frac{2\tilde{e}_i}{d}$.

Claim implies: $\sum_i \mathbb{E}[U_i + 2V_i] < \frac{2}{d}\sum \tilde{e}_i$

$= \frac{2}{d}(\#\text{errors}) < D)$

<u>Proof of Claim:</u>

Two cases based on whether i^{th} block has been decoded correctly by Dec_{in}

Case (i) $X_i = Z_i$

Now, $V_i = 0$ $\quad e_i = \tilde{e}_i$

$$\mathbb{E}[U_i] = \frac{2e_i}{d} = \frac{2\tilde{e}_i}{d} \quad \checkmark$$

Case (ii) $X_i \neq Z_i$

Here, $e_i + \tilde{e}_i \geq d$

$$\left.\begin{aligned} \mathbb{E}[U_i] &= \frac{2e_i}{d} \\ \mathbb{E}[V_i] &= 1 - \frac{2e_i}{d} \end{aligned}\right\} \Rightarrow \begin{aligned} \mathbb{E}[U_i + 2V_i] &= 2 - \frac{2e_i}{d} \\ &= 2\left(1 - \frac{e_i}{d}\right) \\ &\leq \frac{2\tilde{e}_i}{d}. \quad \checkmark \end{aligned}$$

$\boxtimes$

Conclusion: GMD decoder decodes from $< \frac{Dd}{2}$ errors in expectation

Reducing Randomness in GMD decoder.

Idea: As the analysis used only linearity of expectation, use common randomness for all the N blocks

Outer Phase

Choose $\theta \in_R [0,1]$

For each $i \in [N]$

(i) $\tilde{z}_i \leftarrow \begin{cases} \text{'?'} & \text{if } \theta < 2e_i/d \\ z_i & \text{otherwise} \end{cases}$

Run Dec_{out} on $(\tilde{z}_1, \tilde{z}_2, \ldots, \tilde{z}_N)$ to obtain $(\tilde{m}_1, \ldots, \tilde{m}_k) \in [Q]^k$.

Further observe that the above alg is unchanged if θ is between two successive $\frac{2e_i}{d}$

Outer Phase

Let $\Theta = \{ \frac{2e_i}{d} \mid i \in [N] \} \cup \{0, 1\}$

For each $\theta \in \Theta$

{ For each $i \in [N]$

(i) $\tilde{z}_i \leftarrow \begin{cases} \text{'?'} & \text{if } \theta < 2e_i/d \\ z_i & \text{otherwise} \end{cases}$

Run Dec_{out} on $(\tilde{z}_1, \tilde{z}_2, \ldots, \tilde{z}_N)$ to obtain $\tilde{m}_\theta$ $(\tilde{m}_1, \ldots, \tilde{m}_k) \in [Q]^k$.

Output $\tilde{m}_{\theta_*}$ st $\theta_* = \underset{\theta \in \tilde{\Theta}}{\arg\min} \; \Delta(C(\tilde{m}_\theta), x)$

Graph based Codes.

Gallagher '63
Tanner '84
Sipser–Spielman '94
Spielman '95

GF(2)- Linear codes.

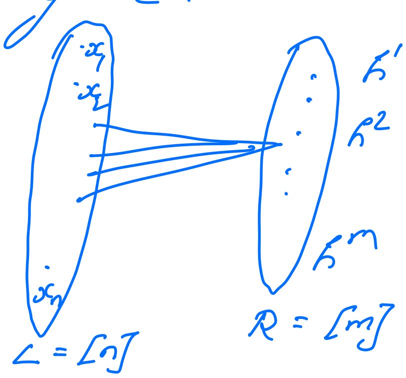
- Parity check matrix representation

$$n-k = m \left\{ \underbrace{\begin{bmatrix} \leftarrow & h^1 & \rightarrow \\ \leftarrow & h^2 & \rightarrow \\ & \vdots & \\ \leftarrow & h^m & \rightarrow \end{bmatrix}}_{H} \right. \overset{\longleftarrow \; n \; \longrightarrow}{} \begin{bmatrix} x \end{bmatrix} \overset{?}{=} 0$$

$$C = \{ x \in \{0,1\}^n \mid Hx = 0 \}.$$

Factor graph of C.

(L, R, E)



– m rows/constraints

$(i,j) \in E$
$\Updownarrow$
$h_i^j \neq 0$

$G = (L, R, E)$

$$C(G) = \{ x \in \{0,1\}^L \mid \forall r \in R, \sum_{\ell \in \Gamma(r)} x_\ell = 0 \}$$

Rate of $C(G)$: $\dim(C(G)) \geq |L| - |R|$
$= n - m$

If $m \leq (1-R)n$, then $\text{Rate}(C(G)) \geq R$.

Gallagher: Restriction attention to bipartite graphs whose right (constraint) degree is bounded.

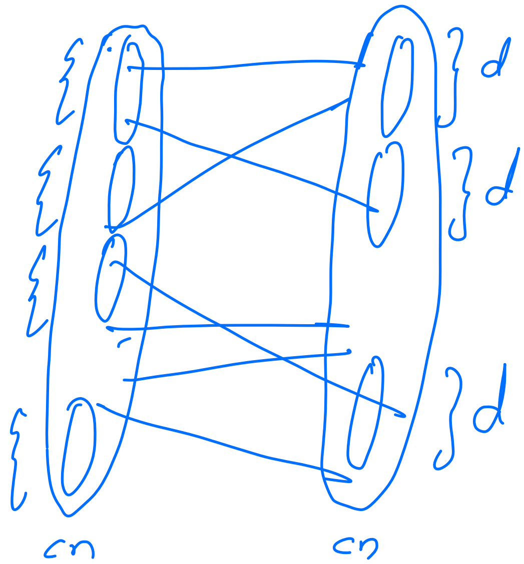
Low - Density Parity Check (LDPC) codes

$G = (L, R, E)$ is (c,d)-regular if the left (variable) degree $= c$ & the right (constraint) degree $= d$.

(c,d)-bounded if left degree $\leq c$
& right - degree $\leq d$.

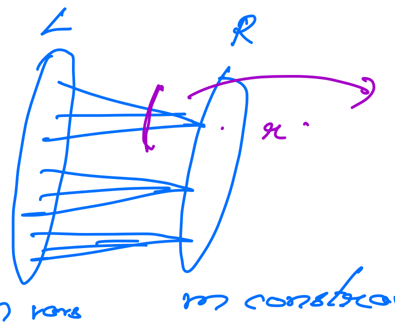
Thm [Gallagher] A random LDPC code (that is obtained by picking a random (c,d)-regular graph) attains the GV bound.

$\sigma : [cn] \to [cn]$ - random permutation



$dm = cn$

Tanner:



$$\sum_{e \in N(r)} x_e = 0$$

Tanner:

$\mathcal{C} \subseteq [d, \ell, \delta d]_2$ - code

$$\mathrm{Tan}(G, \mathcal{C}) = \{ x \in \{0,1\}^L \mid \forall r \in R. \; x|_{N(r)} \in \mathcal{C} \}$$

$$\mathcal{C}(G) = \mathrm{Tan}(G, \mathrm{EVEN})$$

Sipser. Spielman:

Expansion guarantees distance

(i) G is a <u>very good</u> expander

$\Downarrow$

$\mathcal{C}(G)$ has distance.

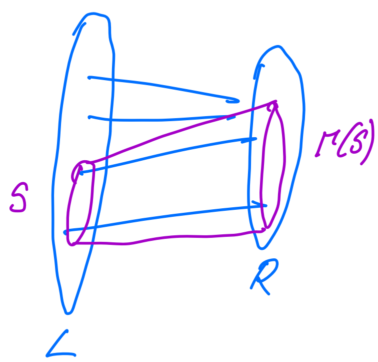
(ii) G is an expander

$\Downarrow$

$Tan(G, \mathcal{C})$ has distance for certain choices of inner code $\mathcal{C}$.

Expander Graphs

$G = (L, R, E)$ $\qquad$ G is (c,d)-bounded.



$|L| = n$ $\qquad$ $|R| = m$

G is (δ, A)-expander if $\forall S \subseteq L$

$$|S| \leq \delta |V| \Rightarrow |\Gamma(S)| \geq A|S|$$

$$\Gamma(S) = \{ j \in R \mid \exists \text{ edge } (i,j) \in E,\ i \in S \}.$$

$$\Gamma^{odd}(S) = \{ j \in R \mid |\Gamma(j) \cap S| = \text{odd} \}.$$

$$\Gamma^{+}(S) = \{ j \in R \mid |\Gamma(j) \cap S| = 1 \}$$

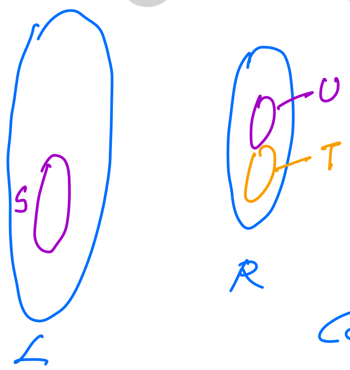
$$\Gamma^{+}(S) \subseteq \Gamma^{odd}(S) \subseteq \Gamma(S).$$

G is a (δ, A)-unique expander if $\forall S \subseteq L$
$|S| \leq \delta |V| \Rightarrow |\Gamma^+(S)| \geq A|S|$

<u>Claim</u>: If $G = (L, R, E)$ is a (δ, A)-expander then it is a $(\delta, 2A - c)$-unique expander where G is (c, d)-regular.

$(A > c/2)$

<u>Pf</u>:



$U = \Gamma^+(S)$

$T = \Gamma(S) \setminus \Gamma^+(S)$

$|U \cup T| \geq A|S|$

Count # edges between S & $\Gamma(S)$

Left side $\leq c|S|$

Right side: $\geq |U| + 2|T|$

$$|U| + 2|T| \leq c|S|$$

$$|U| + 2(|\Gamma(S)| - |U|) \leq c|S|$$

$$|U| \geq 2|\Gamma(S)| - c|S|$$

$$\geq (2A - c)|S|$$

∎

<u>Obs</u>: $G = (L, R, E)$ is a (δ, A^+)-unique expander for any $A^+ > 0$, then $\delta(\mathcal{C}(G)) \geq \delta$.

∎

<u>Cor</u>: $G = (L, R, E)$ is a (δ, A)-expander for

$\Delta > c/2$, then $\delta(\mathcal{C}(G)) \geq \delta$. ∎