April 17, 2019

REMINDERS

(°) Video due in ~ 2.5 weeks (11:59 pm on Tue, Apr 30)

(°) HW 3 will be graded by Tue

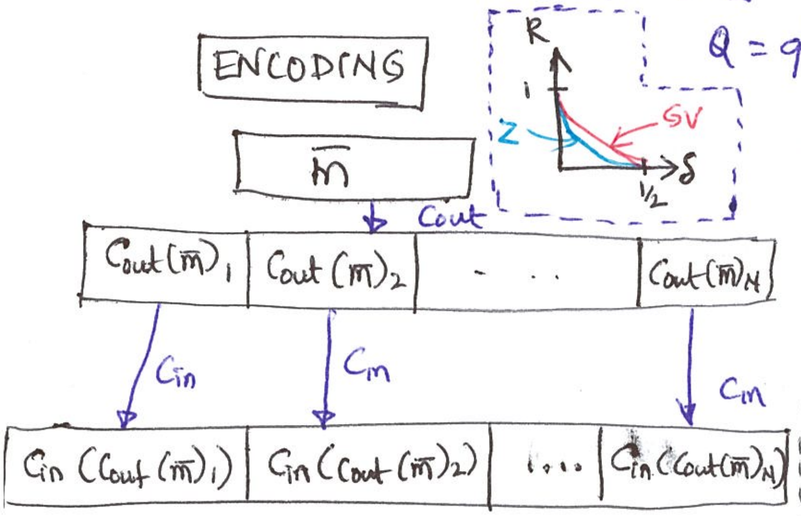
RECAP

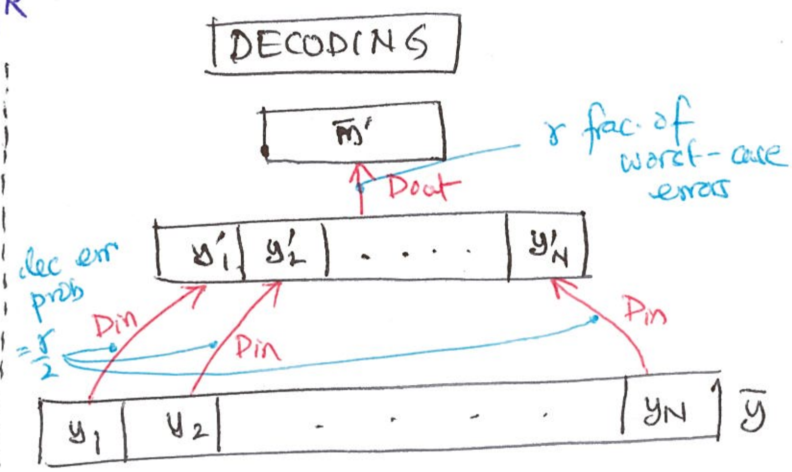
Q: Explicit BSC$_p$ capacity achieving codes with efficient decoding

CODE CONCATENATION

$C_{out} : [Q]^K \to [Q]^N$; $C_{in} : [q]^k \to [q]^n$

$Q = q^k$





	Len	Dim	q	Rate	Decoder	Dec time	Decoding guarantee
C_{out}	N	K	2^k	$1-\frac{\varepsilon}{2}$	D_{out}	$T_{out}(N)$	$\le \gamma$ frac. of WORST CASE error
C_{in}	n	$k = O(\log N)$	2	$1-H(p)-\frac{\varepsilon}{2}$	$D_{in}\ (= MLD_{C_{in}})$	$T_{in}(k)$	Dec error prob $\le \frac{\gamma}{2}$ over BSC$_p$

$C^* = C_{out} \circ C_{in}$ $\qquad \mathcal{N} = Nn$

→ $R(C^*) \ge 1 - H(p) - \varepsilon$

→ Decoding time $= poly(\mathcal{N})$ $\quad$ [assuming $T_{out}(N) = poly(N)$, $T_{in}(k) = 2^{O(k)}$]

Can decode RS codes up to $(1-R)/2$ errors in $O(N^3)$ time

→ Encoding time $= O(\mathcal{N}^2)$

→ Decoding error prob: $2^{-\Omega(\gamma N)}$

TODAY (proofreader: Sai)

(°) Work out C_{in} & C_{out} for final BSC$_p$ cap. achieving codes

(°) Unique decoding algo for RS codes [Welch-Berlekamp algo]

2^{kn} <u>Inner Code</u>: Compute C_{in} by brute force over all

$\to$ $k \times n$ gen matrices. **Ex:** In $2^{O(n)}$ time for every transmitted msg $\bar{m}$ & rcvd word $\bar{y}$, compute the prob that $\bar{y}$ is not decoded to $\bar{m}$ by MLD

$\to$ $\exists$ a linear code of rate $1-H(p)-\frac{\varepsilon}{2}$ that achieves BSCp capacity w/ $2^{-\Theta(\varepsilon^2 n)}$ dec. error prob.

$\Rightarrow 2^{O(n^2)}$ time overall.

$\hookrightarrow \le \frac{\gamma}{2}$

$\Omega\left(\frac{\log\frac{1}{\gamma}}{\varepsilon^2}\right) \le k \le O(\log N)$ $\quad k \ge \Rightarrow n \ge \Omega\left(\frac{\log\frac{1}{\gamma}}{\varepsilon^2}\right)$

$T_{in}(k) = 2^{O(k)}$ since MLD

<u>OUTER CODE</u>: rate $\ge 1-\frac{\varepsilon}{2}$ can correct $\ge \gamma$ frac of errors.

Pick C_{out} of RS of rate $1-\frac{\varepsilon}{2}$ $\Rightarrow$ can correct up to $\frac{\varepsilon}{4}$ frac of error

$T_{out}(N) = O(N^3)$ $\quad$ If $\gamma = \frac{\varepsilon}{4}$.

$n = \Theta(\log N)$

Construction time for C_{in}: $2^{O(n^2)} = 2^{O(\log^2 N)} = N^{O(\log N)}$

We need $\langle$ Explicit C_{out} of rate $1-\frac{\varepsilon}{2}$, correct $\ge \gamma$ frac of worst case errors over alphabet of 2^k, $k = O(\sqrt{\log N})$

$Q = 2^k = 2^{O(\sqrt{\log N})}$

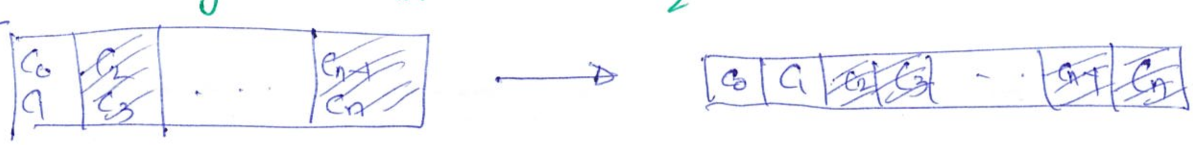
A: Explicit codes on Zyablov bound that can correct γ fract of errors & rate $1-f(\gamma)$ $\to 0$ as $\gamma \to 0$

C'

$\to$ need this for $\Omega\left(\frac{\log\frac{1}{\gamma}}{\varepsilon^2}\right) \le k \le O(\sqrt{\log N})$

$\to$ "Bunch" / "fold" k consecutive bits of codewords in C' to get C_{in} over $\mathbb{F}_{2^k}$

$k=2$



If we have γ frac of errors over $\mathbb{F}_{2^k}$:

$$C': \mathbb{F}_2^{k\cdot K} \to \mathbb{F}_2^{k\cdot N} \equiv C_{in}: \mathbb{F}_{2^k}^K \to \mathbb{F}_{2^k}^N$$

$\bar{y} \in \mathbb{F}_{2^k}^N$ has ρ frac of errors $\Rightarrow$ $\le \rho N$ errors

$\bar{y}' \in \mathbb{F}_2^{kN}$ is "unfolded" version of y

$\bar{y}'$ has $\le \rho N \cdot k$ error $\Rightarrow$ frac of errors in $\bar{y}' \le \frac{\rho N k}{N k} = \rho$ ∎

Our final choice of C_{out}: C' on Zyablov bound $\to$ fold k bits into $\in \mathbb{F}_{2^k}$

$$n \sim k = \Theta\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right)$$

D_{out}: i/p: $\bar{y} = (y_1, \ldots, y_N) \in (\mathbb{F}_{2^k})^N$

1. Unfold $\bar{y}$ to $\bar{y}' \in \mathbb{F}_2^{kN}$
2. Run $\frac{1}{2}$(design distance) decoding algo for C' on $\bar{y}$

Zyablov: dist 2γ with rate $1 - O(\sqrt{\gamma}\log\frac{1}{\gamma}) \ge 1 - \frac{\varepsilon}{2}$

$$\Rightarrow \varepsilon \le O(\sqrt{\gamma}\log\frac{1}{\gamma})$$

$$\ldots \gamma = \varepsilon^3 \checkmark$$

Finally, binary linear code of rate $1-H(p)-\varepsilon$ of block length N

(•) Construct it in time: $\text{poly}(N) + 2^{O(1/\varepsilon^5)}$ $\left[n = O\left(\frac{\log\frac{1}{\varepsilon}}{\varepsilon^2}\right)\right]$

(•) Enc. time $= O(N^2)$

(•) Dec tm $= \text{poly}(N) + N \cdot 2^{O(\frac{1}{\varepsilon^3})}$

(•) Dec error $= 2^{-\Omega(\underbrace{\varepsilon^6}_{\varepsilon^2 \text{ from Shannon.}} \cdot N)}$

N is $2^{\text{poly}(\frac{1}{\varepsilon})}$ Open Q: above $N = \text{poly}(\frac{1}{\varepsilon})$

↳ not open any more! Polar codes,

Last missing piece! Unique decoder of RS codes.

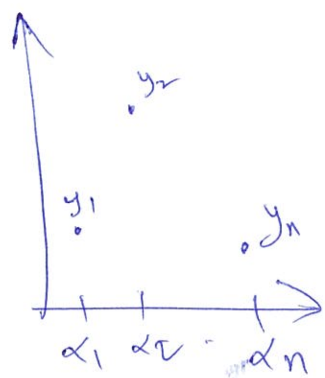
Given $[n, k, d = n-k+1]_q$ RS codes, eval pts $\alpha_1, \dots, \alpha_n$

$q \geq n$

Syntactic change! $\bar{y} = (y_1, \dots, y_n) \in \mathbb{F}_q^n$

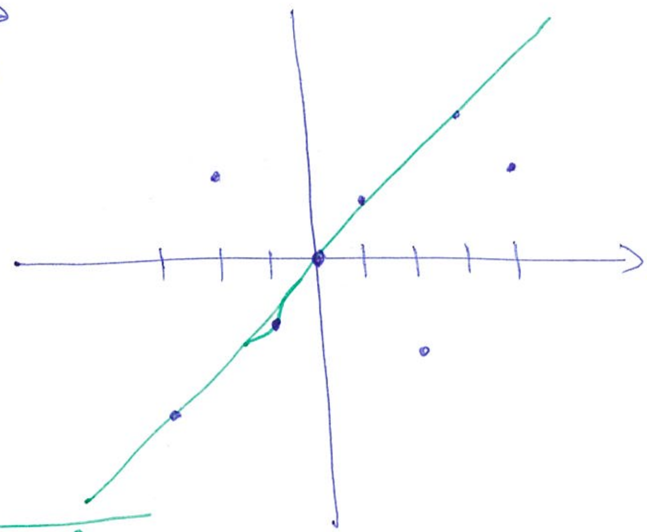
$\equiv (\alpha_1, y_1), (\alpha_2, y_2), \dots, (\alpha_n, y_n)$

$\in (\mathbb{F}_q \times \mathbb{F}_q)^n$



Want: poly $P(X)$ of deg $\leq k-1$ s.t for at least $n-e$ $i \in [n]$

$P(\alpha_i) = y_i$



$n = 8$

$k = 2$

$e < \frac{n-k+1}{2}$

$e = 3$

$e < \frac{n-k+1}{2}$

Welch-Berlekamp algo

(1) Assume you know $P(X)$

(2) Derive some poly identities using $P(X)$ & $\bar{y}$

(3) $\hookrightarrow$ linear equations.

s.t $P(X)$ is a valid solution.

(4.1) Show that can be solved (GE)

(4.2) $P(X)$ is the "only" solution.

We know $P(X)$: $\deg(P) < k$ & $P(\alpha_i) \neq y_i$ for $\leq e$ locations $i \in [n]$

Error locator polynomial: $E(X)$ s.t $\forall i$ w/ $P(\alpha_i) \neq y_i$

$E(\alpha_i) = 0$

$$E(X) = \prod_{\substack{i \\ P(\alpha_i) \neq y_i}} (X - \alpha_i)$$

Claim: $\forall\ i \in [n]$, $y_i\, E(\alpha_i) = P(\alpha_i) \cdot E(\alpha_i)$

Pf: Case 1: $P(\alpha_i) = y_i$

Case 2: $P(\alpha_i) \neq y_i$

monic deg $\leq e$ poly

→ Think of coefficient of $P(X)$ & $E(X)$ as vars

k

e vars.

n equations in $\leq e+k$ vars.

$$k+e < k + \frac{n-k+1}{2} \leq n.$$

BUT quadratic equations