April 9, 2019

REMINDERS

(•) Mini-projects reports have been graded

(•) ALL of the video content should be YOUR OWN.

(•) HW 3 graded by next Tue

(•) Video due in 3 WEEKS (by 11:59pm on Tue, Apr 30)

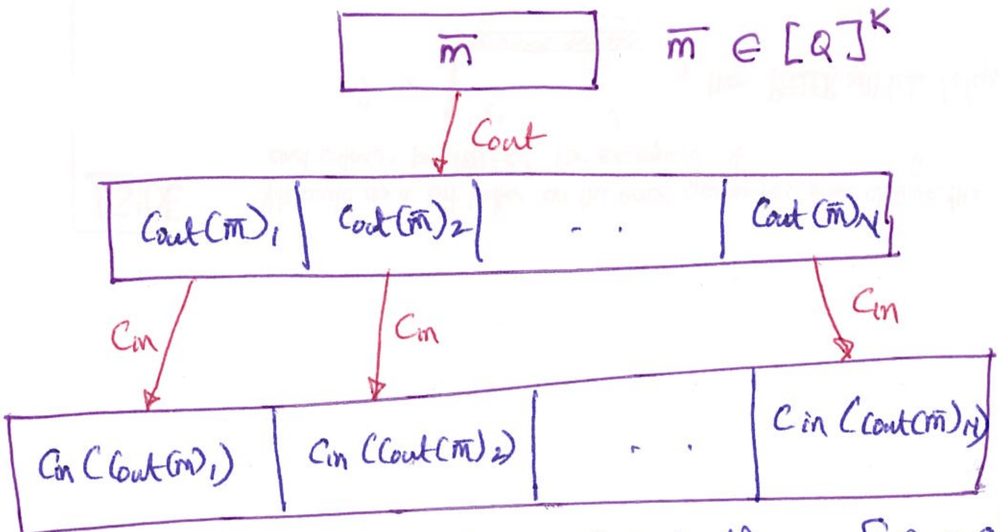
RECAP

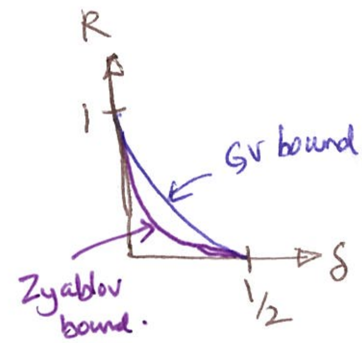
Q: Explicit asymptotically good codes that we can correct from $\rho > 0$ fraction of errors?

Code Concatenation:

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

$C_{in}: [q]^k \to [q]^n$





(•) $C_{out}: (N, K, D)_Q$ $\quad C_{in}: (n, k, d)_q$ $\quad [Q = q^k]$ $\quad$ ($N \geq$ ... $\overset{}{N}$)

$\Rightarrow C_{out} \circ C_{in}$ is $(Nn, Kk, Dd)_q$ code

(•) $\exists$ ~~an~~ explicit (concatenated code) on Zyablov bound

↳ C_{out}: RS code with $N = Q = q^k \Rightarrow k = O(\log_q N)$

↳ C_{in}: Use $q^{O(n)}$ time to get code on GV bound

TODAY [Proof reader: Harsha]

(•) Decoding concatenated code ($< \frac{Dd}{4}$ today. $< \frac{Dd}{2}$ in book)

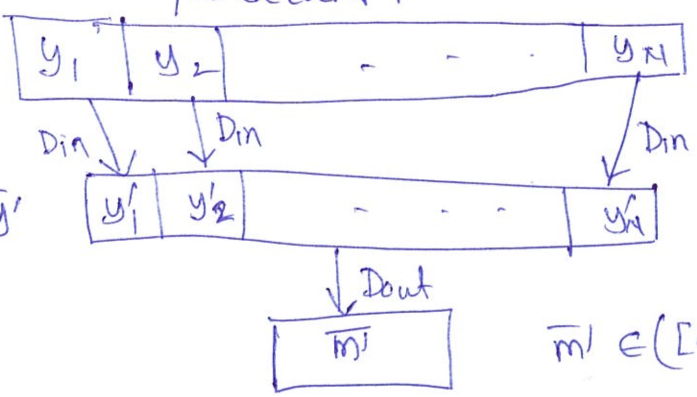
(•) Achieving BSC_p cap with explicit codes & efficient decoding

Assume: $\exists$ a unique decoder of RS codes $\left(\frac{1-R}{2}\right)$ that runs in ~~time~~ $O(N^3)$ ops over $\mathbb{F}_Q$

For $C_{out} \to D_{out}$ $\qquad [N = Q = q^k]$

Q: D_{in} for C_{in}? MLD $\qquad q^{O(k)} = \text{poly}(N)$ $\qquad \boxed{\frac{Dd}{4}}$

$\uparrow$ unique decoder.

$([q]^n)^N \ni \bar{y} =$  $\quad y_i \in [q]^n$

$([Q])^N = (q^k)^N \ni \bar{y}'$ $\quad y'_i \in [q]^n$

$\bar{m}' \in ([q]^k)^K$ $\quad$ (Hope: $\bar{m}' = \bar{m}$ if not too many errors.)

Algo 1: i/p: $\bar{y} = (y_1, \dots, y_N) \in ([q]^n)^N$

o/p: $\bar{m}' \in ([q]^k)^K$

1. $\bar{y}' = (y'_1, \dots, y'_N)$ where $\underbrace{C_{in}(y'_i) = D_{C_{in}}(y_i)}_{\text{poly}(N)}$ $\quad 1 \le i \le N$
2. $\bar{m}' = D_{out}(\bar{y}')$ $\leftarrow O(N^3)$
3. Return $\bar{m}'$ $\qquad \Rightarrow N \cdot \text{poly}(N) + O(N^3) = \text{poly}(N)$ $\qquad$ $\text{poly}(N) \Vert Nn$

Lemma 1: Algo 1 can correct from $< \frac{Dd}{4}$ errors.

Pf: $\bar{m} \in ([q]^k)^K$ s.t. $\Delta(\bar{y}, C_{out} \circ C_{in}(\bar{m})) < \frac{Dd}{4}$

$\uparrow$ why is $\bar{m}$ unique? $\Delta(C_{out} \circ C_{in}) \ge Dd$

Def: Bad event at $i \in [N]$ if $C_{in}(y'_i) \ne C_{in}(C_{out}(\bar{m})_i)$

Claim: If # bad events $< \frac{D}{2} \Rightarrow$ Algo 1 is correct. $\leftarrow$ D_{out} can correct $< \frac{D}{2}$ errors.

Note: If $\Delta(y_i, C_{in}(C_{out}(\bar{m})_i)) < \frac{d}{2} \Rightarrow$ no bad event at i. $\leftarrow$ C_{in} has dist d & b/c MLD.

$\Rightarrow$ bad event at $i \Rightarrow \Delta(y_i, C_{in}(C_{out}(\bar{m})_i)) \ge \frac{d}{2}$

If there are $\ge \frac{D}{2}$ bad events $\Rightarrow \ge \frac{D}{2}$ locations i

$\Delta(y_i, C_{in}(C_{out}(\bar{m})_i)) \ge \frac{d}{2} \Rightarrow \Delta(\bar{y}, C_{out} \circ C_{in}(\bar{m})) \ge \frac{D}{2} \cdot \frac{d}{2} = \frac{Dd}{4}$

COR: Can correct up to $\frac{1}{4}$ · Zyablov bound in poly(N) time

Q: Can we efficiently decode up to $\frac{1}{2}$ Dd? (12.2 + 12.3 in book)

Efficiently achieving BSC$_p$ capacity

$q = 2$

	Shannon	Hamming: Unique	Hamming: List
Capacity	$1 - H(p)$	R vs. δ [MRRW, GV]	$1 - H(p)$
Explicit codes	?	Zyablov bound	?
Efficient algo	?	$\frac{1}{2}$ · Zyablov bound	?

YES! via concatenated codes

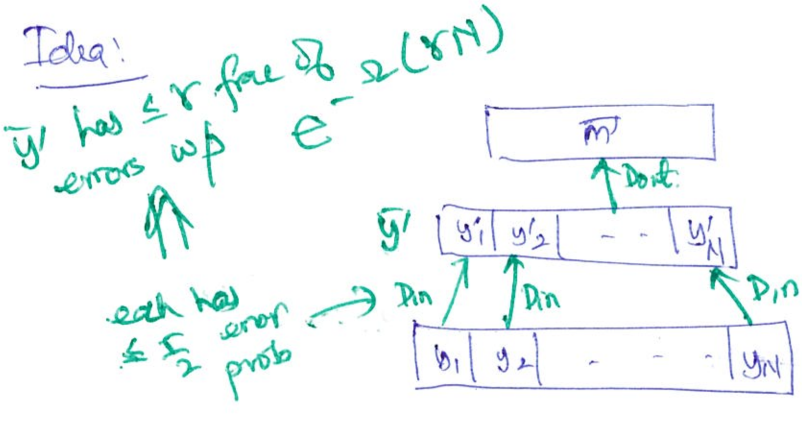
NO one knows ($q > 2$)

Q: C_{in}? BSC$_p$ capacity achieving code

(~~Fun~~ Fun fact: Linear codes on cap. w/ decoding error $2^{-\Theta(\varepsilon^2 n)}$ ↳ $1 - H(p) - \varepsilon$

C_{out}? → RS codes (correct const frac. of worst-case errors)

Idea:



Pick parameters s.t. dec. error prob for C_{in} $(2^{-\Theta(\varepsilon^2 n)})$ $\le \frac{\gamma}{2}$

Notation params: $N = 2^k$

	Length	Dim	q	Rate	Decoder	Dec. time	Decoding guarantee
C_{out}	N	K	2^k	$1-\varepsilon/2$	D_{out}	$T_{out}(N)$	$\leq \gamma$ frac of worst-case errors
C_{in}	n	$k = O(\log N)$	2	$1-H(p)-\frac{\varepsilon}{2}$	$D_{in} = MLD_{C_{in}}$	$T_{in}(k)$	$\leq \frac{\gamma}{2}$ error prob over BSC_p

→ $C^* = C_{out} \circ C_{in}$

$R(C^*) \geq \left(1-\frac{\varepsilon}{2}\right)\left(1-H(p)-\frac{\varepsilon}{2}\right) \geq 1-H(p)-\varepsilon$

$\mathcal{N} = Nn$ $\quad$ p is constant $\quad$ $n = \Theta(k)$

→ Decoding ~~time~~ algo: Algo 1 doesn't change.

→ Decoding time: $N \cdot \underbrace{T_{in}(k)}_{2^{O(k)}} + \underbrace{T_{out}(N)}_{poly(N)} \leq poly(\mathcal{N})$

→ Encoding time: $N \cdot O(n^2) + O(N^2 \cdot k^2)$ ← N^2 ops over $\mathbb{F}_{2^k}$

$= O(\mathcal{N}^2)$

Decoding error prob: Fix $1 \leq i \leq N$ $\Pr[y'_i \neq C_{out}(\bar{m})_i] \leq \frac{\gamma}{2}$

Note: each decoding error is independent for each i.

$\Rightarrow$ By chernoff bound, Prob $> \gamma N$ ~~er~~ dec errors (i.e $y'_i \neq C_{out}(\bar{m})_i$) is $e^{-\frac{\gamma N}{6}}$

$\propto 2^{-\Omega\left(\frac{\gamma \mathcal{N}}{n}\right)}$ ← final decoding error prob.