Apr 13

REMINDER

(∘) HW 5 due tonight at 11:59 pm
(∘) HW 6 (last HW!) out by tonight at 11:59pm
↳ If you plan to drop HW 5+6, please do NOT submit!
(∘) Video due in 4 weeks (11:59pm, Wed, May 11)
↳ Please take my comments + grading rubric into account!

RECAP

$q=2$

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

still open for $q=2$

YES! via concat codes

(∘) Code concatenation: D_{out} $(D/2)$ $\{ C_{out} : [Q]^K \to [Q]^N$ $\quad Q = q^k$

$\bar{m} \in [Q]^K$ unique decoder → D_{in} $(d/2)$ $\{ C_{in} : [q]^k \to [q]^n$

$C_{out} \circ C_{in}(\bar{m}) = (C_{in}(C_{out}(\bar{m})_1), \ldots, C_{in}(C_{out}(\bar{m})_N))$

(∘) Algo 1: input: $\bar{y} = (y_1, \ldots, y_N) \in ([q]^n)^N$

1. $\bar{y}' \leftarrow (y'_1, \ldots, y'_N)$ where $C_{in}(y'_i) = D_{in}(y_i)$ $\forall i \in [N]$
2. $\bar{m}' \leftarrow D_{out}(\bar{y}')$
3. Return $\bar{m}'$

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

TODAY!

(∘) Proof readers: ~~[illegible]~~ Ning, Eshan
(∘) Proof of Lemma
(∘) Using code concat to achieve BSC$_p$ capacity (with efficient algos!)

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

This $\bar{m}$ is unique since dist of $C_{out} \circ C_{in} \geq Dd$

Prove: Algo 1 given $\bar{y}$, outputs $\bar{m}$

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

(if not bad event $\Rightarrow y'_i = C_{out}(\bar{m})_i$

Claim1: If # bad events $< \frac{D}{2} \Rightarrow$ Algo 1 is correct

(Dout can correct from $< \frac{D}{2}$ errors)

Claim2: # bad events $< \frac{D}{2}$

(Claim 1+2 $\Rightarrow$ Lemma)

Pf: For contradiction assume # bad events $\geq \frac{D}{2}$

Bad event at $i \in [N]$, $\Delta(y_i, \cancel{C_{out} \circ C_{in}(\bar{m})}$ $C_{in}(C_{out}(\bar{m})_i)) \geq \frac{d}{2}$

Because: if not

$\Delta(y_i, C_{in}(C_{out}(\bar{m})_i)) < \frac{d}{2}$

$\Rightarrow$ since Din does unique decoding, $y'_i = C_{out}(\bar{m})_i$

$\Rightarrow \Delta(\bar{y}, C_{out} \circ C_{in}(\bar{m})) \geq \frac{D}{2} \cdot \frac{d}{2} = \frac{Dd}{4}$ contradiction to (*) ∎

COR: Correct upto $\frac{1}{4} \cdot$ Zyablov bound in poly(N) time.

Q: Can we get the same result for $\frac{1}{2} \cdot$ Zyablov bound?

YES (13.2 + 13.3 in the book)

Achieving BSCp capacity w/ efficient codes + efficient algo

→ Via concatenated codes

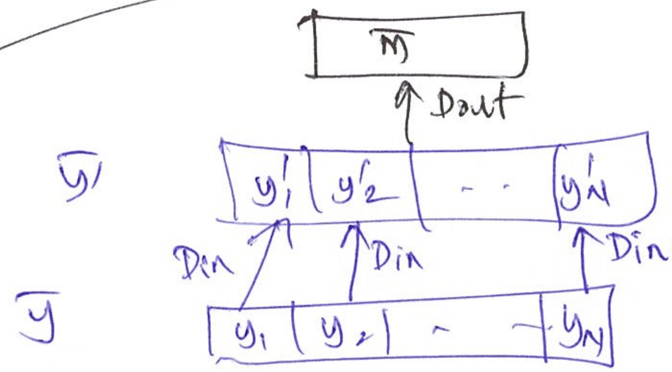
Cout? RS codes (correct const. frac of worst-case errors)

Cin? BSCp capacity achieving code

(Fun fact: ∃ linear codes of rate $1-H(p)-\varepsilon$ w/ decoding error prob $2^{-\theta(\varepsilon^2 n)}$

via MLD

Overall idea:



each dec. error prob is independent.

each has decoding error prob of $\le \frac{\gamma}{2}$

$\Rightarrow$ Use chernoff to argue that frac of errors $< \gamma N$ (Din failed at loc $i \in [N]$) is $e^{-\Omega(\gamma N)}$

$\Rightarrow$ $< \gamma N$ fraction of errors for Dout

Good if Dout can handle $< \gamma$ frac of worst-case errors

Parameter table! (What we want / ideal Cout / Cin) $N = 2^k$

	Length	Dim	q	Rate	Decoder	Dec time	Decoding guarantee
Cout	$N=2^k$	K	2^k	$\ge 1-\varepsilon/2$	Dout	$T_{out}(N)$ $\le poly(N)$	$\le \gamma$ frac of worst-case errors
Cin	n	$k=\log_2 N$	2	$\ge 1-H(p)-\frac{\varepsilon}{2}$	Din = MLD_{Cin}	$T_{in}(k)$	$\le \frac{\gamma}{2}$ dec error prob over BSC_p

Assume we have the above,

→ $C^* = C_{out} \circ C_{in}$

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

$\mathcal{N} = Nn$, p is const $\Rightarrow n = \Theta(k)$

→ Decoding algo: Same as Algo 1.

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

→ Enc. time: $N \cdot O(n^2) + O(\underbrace{N^2}_{O(N^2) \text{ ops over } \mathbb{F}_{2^k}} \cdot k^2)$ $\le O(\mathcal{N}^2)$

op time for $+, -, *, \div$ over $\mathbb{F}_{2^k}$

→ Dec. error prob: $\forall i \in [N]$, $\Pr[y'_i \neq \mathrm{Cout}(\bar{m})_i] \leq \frac{\gamma}{2}$

⇒ By Chernoff, prob of $> \gamma N$ decoding error i.e. $y'_i \neq \mathrm{Cout}(\bar{m})_i$

is $e^{-\gamma N/6} \leq 2^{-\Omega(\gamma N)}$

If frac of errors $< \gamma$ ⇒ Dout works

$2^{-\Omega(\gamma \frac{N}{n})} \equiv 2^{-\Omega(\gamma \frac{N}{\log N})}$