|Apr 21|

1 min checkin

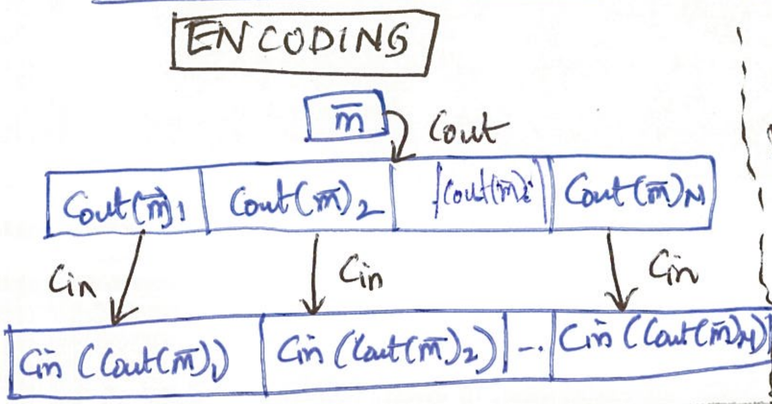
REMINDER

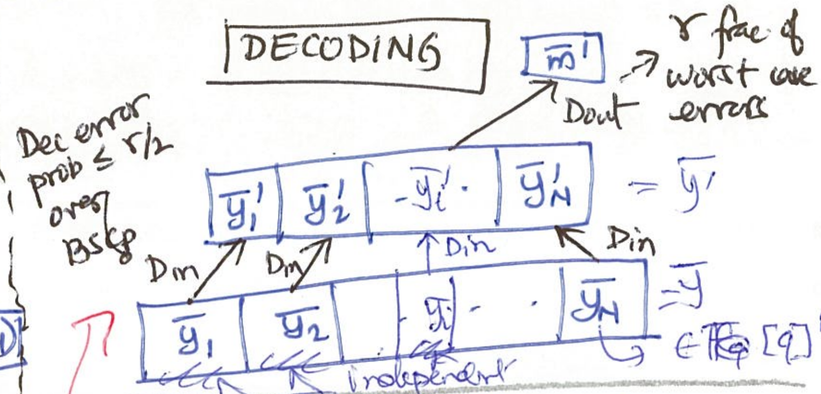
(•) Video due last Sunday of semester (May 14) at 11:59pm
↳ Peer survey due same time

RECAP

(•) Explicit BSC_p capacity achieving linear codes & w/ efficient decoding?

(•) CODE CONCATENATION $C_{out}: [Q]^K \to [Q]^N$, $C_{in}: [q]^k \to [q]^n$, $Q = q^k$





Goal for today (•) Analyze parameters (•) Instantiate C_{in} and C_{out}

Parameter table (what we want / ideal C_{out}/ C_{in}) $N = 2^k$

$q = 2$

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

Assume we have C_{out} & C_{in} as above

$N = 2^k$
$2^{O(k)} \to N^{O(1)}$

→ final code $C^* = C_{out} \circ C_{in}$

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

$\mathcal{N} = Nn$, p is const ⇒ rate of C_{in} is const ⇒ $n = \Theta(k)$

→ Decoding algo: same as Algo 1 from Wed

→ Decoding time: $N \cdot T_{in}(k) + T_{out}(N) \le poly(N)$

$2^{O(k)}$ ↳ $n = \Theta(k)$ ↳ poly(N)

poly(N)

→ Encoding time: $O(\cancel{N^2})$ $O(N^2)$

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

Since BSC_p error for each $i \in [N]$ is independent, we can apply Chernoff

$\Rightarrow$ The prob $> \gamma N$ dec errors (we $> \gamma N$ indices $i \in [N]$ s.t. $\bar{y}_i' \neq (\text{out}(\bar{m}))_i$)

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

C_{in}: BSC_p capacity achieving code.

We know $\exists$ such a code via a gen matrix in $\mathbb{F}_2^{k \times n}$

→ Brute force through all 2^{kn} matrices $\Rightarrow 2^{O(n^2)}$

Overall $2^{O(n^2)} \cdot 2^{O(n)} \cdot 2^{O(n)} = 2^{O(n^2+n)} = 2^{O(n^2)}$

EX 1: In $2^{O(n)}$ time check if for any $G \in \mathbb{F}_2^{k \times n}$ if the max dec error prob $\leq \frac{\gamma}{2}$

↳ EX 0: For any $\bar{m} \in \mathbb{F}_2^k$, $\bar{y} \in \mathbb{F}_2^n$, compute the decoding error prob when $C_{in}(\bar{m})$ was transmitted & $\bar{y}$ was received.

THM: $\exists$ a linear code of rate $1 - H(p) - \frac{\varepsilon}{2}$ that achieves BSC_p capacity with dec err $\leq 2^{-\Theta(\varepsilon^2 n)}$

$$2^{-\Theta(\varepsilon^2 n)} \leq \frac{\gamma}{2} \Rightarrow n \geq \Omega\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right)$$

$$\equiv 2^{\varepsilon^2 n} \geq \frac{2}{\gamma}$$

$$\Rightarrow \varepsilon^2 n \geq \log \frac{2}{\gamma}$$

$$\equiv n \geq \log \tfrac{2}{\gamma} / \varepsilon^2$$

Otoh $k = \log N$

$n \sim k$

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

Construction time: $2^{O(n^2)}$

OUTER CODE: $R \geq 1 - \frac{\varepsilon}{2}$, can correct $< \gamma$ frac. of worst case errors.

(TBD: Relationship b/w ε & γ)

Pick RS code of rate $1 - \frac{\varepsilon}{2} \Rightarrow \delta = \frac{\varepsilon}{2} \Rightarrow \leq \frac{\varepsilon}{4}$ frac. of errors

↳ over $\mathbb{F}_{2^k}$ $\Rightarrow \gamma = \frac{\varepsilon}{4}$

$T_{out} = O(N^3)$ $k = \log_2 N$, $n \sim k$, $n = \Theta(\log N)$

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

$= \left(2^{\log_2 N}\right)^{O(\log N)} = N^{O(\log N)}$!!

In RS code ~~N~~ $Q = 2^k \geq N$ we'll pick $N = 2^k$

$\Rightarrow k \geq \log_2 N$

<u>Fix!</u> We need explicit C_{out} $Q = 2^k$ of rate $1 - \frac{\varepsilon}{2}$ that can correct $< \gamma$ frac of worst case errors.

$k \sim n$ $\quad \Omega\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right) \leq n \leq O\left(\sqrt{\log N}\right)$

$\Rightarrow 2^{O(n^2)} \leq 2^{O\left(\left(\sqrt{\log N}\right)^2\right)} = 2^{O(\log N)} = N^{O(1)}$.

$\equiv \Omega\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right) \leq k \leq O\left(\sqrt{\log N}\right)$

$\hookrightarrow$ We need explicit asymptotically good code over alphabets of size $2^{O(\sqrt{\log N})}$

$\rightarrow$ We've seen such codes over Zyablov bound.

$\hookrightarrow$ <u>Binary codes</u> that can correct γ frac of worst case errors with rate $1 - O\left(\sqrt{\gamma} \log \frac{1}{\gamma}\right)$.

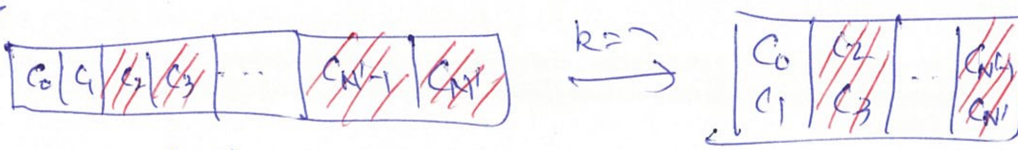
We want codes over $\{0,1\}^k$

<u>Q:</u> Can we convert binary codes to codes on $\{0,1\}^k$ with similar property?

A: Yes! "Fold" / "Bunch" / "Collapse" k bits together.

eg. Let C' be a binary code on the Zyablov bound.

$k = 2$



$C' : \mathbb{F}_2^{k \cdot K} \rightarrow \mathbb{F}_2^{k \cdot N} \in C'$ $\xrightarrow{k \text{ fu}}$ $C_{out} : \left(\mathbb{F}_{2^k}\right)^K \rightarrow \left(\mathbb{F}_{2^k}\right)^N$

<u>Claim:</u> γ frac of error over $\mathbb{F}_{2^k} \Rightarrow \gamma$ frac of error over $\mathbb{F}_2$

(Final) outer : $k = \Theta\left(\log \frac{1}{\gamma} / \varepsilon^2\right)$ Pick a code on Zyablov bound of $k \cdot K$, $k \cdot N$

$\hookrightarrow$ fold it k times