Apr 15

REMINDERS

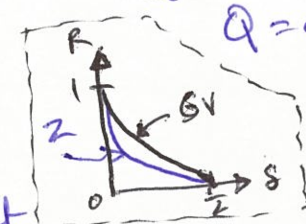
(•) HW6 due by 11:59pm on Wed

RECAP:

Q: Explicit BSC_p capacity achieving codes w/ efficient decoding

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

$Q = q^k$



ENCODING

$\bar{m}$

$\xrightarrow{C_{out}}$

$C_{out}(\bar{m})_1$	$C_{out}(\bar{m})_2$	...	$C_{out}(\bar{m})_N$

$\downarrow C_{in}$

$C_{in}(C_{out}(\bar{m})_1)$	$C_{in}(C_{out}(\bar{m})_2)$	...	$C_{in}(C_{out}(\bar{m})_N)$

DECODING

$\bar{m}'$

$\uparrow D_{out}$ — γ frac. of worst case errors

y_1'	y_2'	...	y_N'

$\uparrow D_{in}$ — dec error prob on BSC_p $\leq \frac{\gamma}{2}$

y_1	y_2	...	y_N

$\bar{y}$

	Len	Dim	q	Rate	Decoder	Dec time	Decoding guarantee
Cout	N	K	2^k	$1-\frac{\varepsilon}{2}$	Dout	$T_{out}(N)$	$\leq \gamma$ frac. of worst-case error
Cin	n	$k = O(\log N)$	2	$1-H(p)-\frac{\varepsilon}{2}$	Din	$T_{in}(k)$	Dec error prob $\leq \frac{\gamma}{2}$ over BSC_p

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

→ $R(C^*) \geq 1 - H(p) - \varepsilon$

→ Decoding time $= poly(\mathcal{N})$ $\Big\{$ assuming $T_{out}(N) = poly(N)$ $\Big\}$

Will show (next week): can decode RS codes up to $\frac{1-R}{2}$ frac of error in $O(N^3)$ ops

→ Encoding time $= O(\mathcal{N}^2)$

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

TODAY

(•) Proof readers: Zhenyi, Imon

(•) Work out instantiations of Cout and Cin

(•) (If there is time) Unique decoder for RS codes [Welch-Berlekamp algo]

C_{in}: ^{BSC_p}Capacity achieving code

Brute force search over all 2^{kn} matrices

Ex: In $2^{O(n)}$ time you can check if a $G \in \mathbb{F}_2^{k\times n}$ is capacity achieving

$\hookrightarrow$ Ex 0.5: for any $\bar{m} \in \mathbb{F}_2^k$ & $\bar{y} \in \mathbb{F}_2^n$ compute the decoding error prob. in $2^{O(n)}$ time

$2^{O(kn)}$ time

THM: $\exists$ a linear code of rate $1 - H(p) - \frac{\varepsilon}{2}$ that achieves BSC_p capacity w/ dec error prob

$$\le 2^{-\theta(\varepsilon^2 n)} \le \frac{\gamma}{2} \Rightarrow n \ge \Omega\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right)$$

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

Construction time $2^{O(n^2)}$, $T_{in}(k) \le 2^{O(k)} = \mathrm{poly}(N)$

OUTER CODE: rate $\ge 1 - \frac{\varepsilon}{2}$, can correct $\le \gamma$ frac of worst-case errors.

(TBD: relation b/w ε & γ).

Pick RS over $\mathbb{F}_{2^k}$ of rate $1 - \frac{\varepsilon}{2} \Rightarrow \delta = \frac{\varepsilon}{2} \Rightarrow \le \frac{\varepsilon}{4}$ frac of errors

$\gamma = \frac{\varepsilon}{4}$!

$T_{out}(N) = O(N^3)$ $k \sim n = \theta(\log N)$ $\{N = 2^k\}$

$\hookrightarrow$ construction of $C_{in} = 2^{O(n^2)} = 2^{O(\log^2 N)} = \left(2^{\log N}\right)^{O(\log N)} = N^{O(\log N)}$

$\Rightarrow$ We need explicit C_{out} $Q = 2^k$ of rate $1 - \frac{\varepsilon}{2}$ & $\le \gamma$ frac of worst case errors w/ $\boxed{\Omega\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right) \le n \le O(\sqrt{\log N})}$

$\Rightarrow Q \approx 2^{O(\sqrt{\log N})}$

for RS code $Q = 2^k \ge N \Rightarrow k \ge \Omega(\log N)$

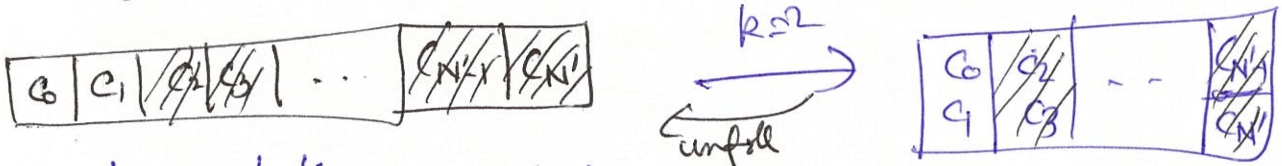
Q: Do we know of explicit codes (over smaller alphabet) that can correct > 0 ~~frac~~ frac. of errors?

A: Yes, Zyablov bound!

↳ Binary alphabet, can correct γ frac of errors w/ rate $1 - O(\sqrt{\gamma}\log\frac{1}{\gamma})$ in poly time

→ "Fold"/"Bunch"/"Group" k consecutive bits into one symbol

C' on ~~Zybol~~ Zyablov bound



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

Claim: γ fraction of errors over $\mathbb{F}_{2^k} \Rightarrow \gamma$ frac of errors over $\mathbb{F}_2$

(FINAL) Outer code: Recall $\Omega\left(\frac{\log\frac{1}{\gamma}}{\varepsilon^2}\right) \leq k \leq O(\sqrt{\log N})$

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

Pick a code C' on the Zyablov bound of blocklength $N\cdot k$ → fold by k to get final C_{out}.

Dout: i/p: $(y_1, \ldots, y_N) \in \mathbb{F}_{2^k}^N$

1. Unfold $\bar{y}$ to $\bar{y}' \in \mathbb{F}_2^{k\cdot N}$
2. Run $\frac{1}{2}$(Zyablov ~~b~~ bound) decoding algo for $\bar{C}'$ on $\bar{y}'$

Recall: Zyablov bound rel dist 2γ w/ rate $1 - O(\sqrt{\gamma}\log\frac{1}{\gamma})$

We need $1 - O(\sqrt{\gamma}\log\frac{1}{\gamma}) \geq 1 - \frac{\varepsilon}{2}$

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

Pick $\gamma = \varepsilon^3$ works. $\Rightarrow k \sim n = O\left(\frac{\log\frac{1}{\varepsilon}}{\varepsilon^2}\right) = O\left(\frac{1}{\varepsilon^3}\right)$

Finally, we get binary linear code of rate $1-H(p)-\varepsilon$ of block length $\mathcal{N} = Nn = O\left(N \cdot \frac{\log \frac{1}{\varepsilon}}{\varepsilon^2}\right) = O\left(2^{k} \frac{\log \frac{1}{\varepsilon}}{\varepsilon^2}\right)$

$= 2^{O(k)}$

$= 2^{O(\frac{1}{\varepsilon^3})}$

(·) Construction time

$C_{in}: \ 2^{O(n^2)} = 2^{O(1/\varepsilon^6)}$

$C_{out}: \ \text{poly}(\mathcal{N})$

} overall $\text{poly}(\mathcal{N}) + 2^{O(\frac{1}{\varepsilon^6})}$

$= \mathcal{N}^{\text{poly}(\frac{1}{\varepsilon})}$

(·) Enc time: $O(\mathcal{N}^2)$

(·) Dec time: $\text{poly}(\mathcal{N}) + N \cdot \underbrace{2^{O(k)}}_{2^{O(1/\varepsilon^3)}}$

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

$= 2^{-\Omega(\varepsilon^6 \mathcal{N})}$

$\gamma N = \frac{\gamma \mathcal{N}}{n}$

$\leq O(\varepsilon^6 \mathcal{N})$

$\mathcal{N} = 2^{\text{poly}(\frac{1}{\varepsilon})}$

Q: $\mathcal{N} \longrightarrow \text{poly}(\frac{1}{\varepsilon})$?

Yes! Polar codes