March 26, 2019

REMINDERS

(•) HW 3 due on Th (11:59pm)

(•) Miniproject report due next Tue (11:59pm)

↳ If you submit your report by Th (& let me know), I'll grade it / give ~~feedback~~ feedback by the weekend. Else I'll grade it after due date.

(•) Please fill in mid-term course evals

(•) HW 2 has been graded

RECAP:

(•) BSC_p : each bit independently gets flipped with prob p

(•) ~~Shanor~~ Shannon's capacity thm ⇒ Capacity $C = 1 - H(p)$ [optimal tradeoff for big Q]

→ Encoder E is random.

→ $D = MLD$

⇒ ① $R < C$ ⇒ exp small decoding prob

② $R > C$ ⇒ at least one message has dec. error prob $\geq \frac{1}{2}$.

⇒ for BEC_α, capacity $= 1 - \alpha$ (Q2 on HW 3).

(•) Our proof only shows ∃ general code that achieves capacity.

Q: Can linear codes achieve BSC_p capacity?

A: Yes (Ex 6.4)

TODAY (Proof reader: Yichen)

(•) ~~Hamming vs~~ Follow up Qs to Shannon's result.

(•) Hamming vs. Shannon

↳ Qualitative

↳ Quantitative

(•) List decoding

Two issues with Shannon's result (even with linear codes):

→ Codes are not "explicit"

→ Decoding time is exponential

Ex: RS is strongly explicit.

<u>Def:</u> (Linear) code is explicit if ∃ a poly time algo to compute a generator matrix.

<u>Def</u> Linear code is <u>strongly explicit</u> if given $(i,j) \in [k] \times [n]$, can compute $G_{i,j}$ in poly$(\log n)$ time.

Q1: Can we get a (strongly) explicit construction of codes with poly time decoding + encoding that achieves BSC_p capacity?

Q2: Above but with $R>0$, $p>0$? (Ex. 6.13)

Hamming vs. Shannon (Qualitative)

Hamming	Shannon
Focus on codewords	Directly deals w/ encoding + decoding
Explicit Codes	Not ~~explicit~~ explicit at all
R v δ	R vs "error parameter"
Worst-case errors	memoryless stochastic errors

Obs: Code can handle $(p+\varepsilon)$-frac of worst-case errors
$\Rightarrow$ reliable communication over BSC_p.

↳ By chernoff bound, Prob $> (p+\varepsilon)n$ errors is $e^{-\varepsilon^2 n/2}$.

Converse (Ex 22) exp small decoding error prob w/ C
$\Rightarrow$ C is rel ~~re~~ dist $\Omega(1)$.

Quantitative Hamming vs. Shannon (large q)

Hamming: $\leq \frac{\delta}{2}$ frac of errors. By Singleton bound $\delta \leq 1-R$

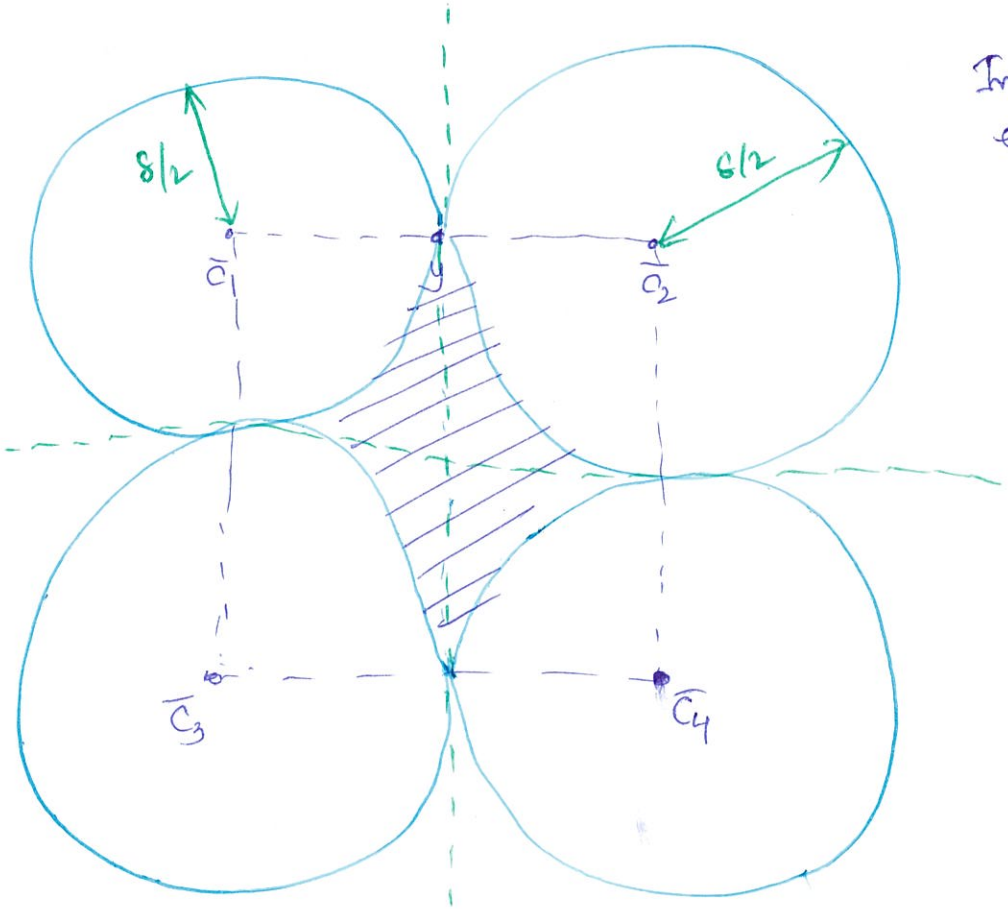
$\Rightarrow P_{Ham} \leq \frac{1-R}{2}$.

→ **Shannon:** qSC_p : Capacity $1-H_q(p)$

It can be shown: $1-p-\varepsilon \leq 1-H_q(p) \leq 1-p$
$q \geq 2^{\Omega(1/\varepsilon)}$

$\Rightarrow P_{Shan} \geq 1-R-\varepsilon$ is possible

Can correct up to twice as many errors in Shannon's setting



In ▨ without ⋮ every received word has a unique closest by codeword.

but we're not decoding these.

$\boxed{q=2}$

Volume of all Hamming balls $= 2^k \cdot \mathrm{Vol}_2\left(\frac{\delta}{2}n, n\right) \le 2^k \cdot 2^{H(\frac{\delta}{2})\cdot n}$

$\Rightarrow$ Empty space ratio $\geq 1 - \dfrac{2^k \cdot 2^{H(\frac{\delta}{2})\cdot n}}{2^n}$.

By Hamming bound

$R \le 1 - H\left(\frac{\delta}{2}\right)$

$R = 1 - H\left(\frac{\delta}{2}\right) - \gamma$

$$= 1 - 2^{Rn} \cdot 2^{-n(1-H(\delta/2))}$$

$$= 1 - 2^{-n(1-H(\delta/2)-(1-H(\delta/2)-\gamma))}$$

$$= 1 - 2^{-\gamma n}.$$

We know if

(1) Deal w/ worst case errors ; AND $\rightarrow$ Shannon's setup: relax this!

(2) Always output the transmitted message/codeword $\Rightarrow \le \delta/2$ errors

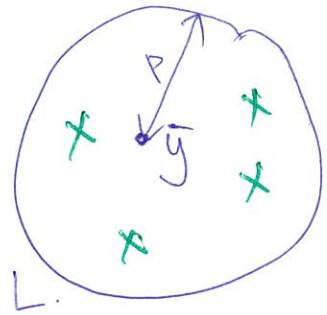
unique decoding

Next: relax this!

List decoding (Elias + Wozencraft late 50s)

Def: $0 \le p \le 1$, $L \ge 1$, $C \subseteq \Sigma^n$ is (p, L) list decodable if $\forall\, \bar{y} \in \Sigma^n$

$$|\{C \cap B(\bar{y}, pn)\}| \le L$$



$\#\times \le L$

$$\equiv \quad |\{\bar{c} \in C \mid \Delta(\bar{y}, \bar{c}) \le pn\}| \le L.$$

Q: If C has rel distance δ, C is $(< \frac{\delta}{2}, 1)$-list decodable

$\Rightarrow$ (p, L)-l.d. C $\Rightarrow$ for any transmitted codeword/msg $\bar{m}$, if we have $\le p$ frac. of errors $\Rightarrow$ combinatorially, $\bar{m}$ is in a list of size $\le L$

$\Rightarrow$ poly time list decoder, $L \le \text{poly}(n)$

Want: L to be $\text{poly}(n)$.

What to do with lists of size > 1.

(•) Declare an error!
↳ random errors whp Hamming balls of radius $\delta - \varepsilon$ have ≤ 1 codeword (Sec 7.5)

(•) If $\exists$ side information $\Rightarrow$ $O(\log L)$ bits of information suffice!

Q3: Can we correct $> \frac{\delta}{2}$ errors w/ list size $\text{poly}(n)$

Q4: What is the max frac of errors w/ l.d. & $L = \text{poly}(n)$