Mar 28

REMINDERS:

(∘) Mini-project 2 pg. report due by 11:59 pm on Wed
↳ ALL group members INDIVIDUALLY submit SAME PDF.

(∘) New HW grade policy is now in place! (50 Yes, 2 DC, 0 No)

(∘) Proof readings for rest of semester finalized
↳ Please check the schedule page for your assigned lecture

RECAP

(∘) BSC_p: each bit independently gets flipped w/ prob p

(∘) Shannon's capacity thm $\Rightarrow$ for BSC_p capacity $C = 1 - H(p)$

(∘) Encoder E: random

(∘) $D = MLD_E$

↳ ① $R < C \Rightarrow$ exponential small dec error prob

② $R > C \Rightarrow$ at least one message has decoding error prob $\geq \frac{1}{2}$

↳ for BEC_α, capacity $= 1 - \alpha$ (Ex. 6.7 in book)

(∘) Our proof only shows $\exists$ general code that achieves capacity

Q: Can linear codes achieve BSC_p capacity?

A: Yes (Ex 6.4 in the book)

TODAY

(∘) Proof reader: Henry

(∘) Follow up Qs to Shannon's result → Qualitative

(∘) Hamming vs. Shannon ⟷ Quantitative

(∘) List decoding (if there's time)

Two issues w/ Shannon's result (even w/ linear codes)

(→) Codes are not "explicit"

(→) Decoding time is exponential

Def: (Linear) code C is explicit, if $\exists$ a poly time (poly(n)), given k, n) to compute a $k \times n$ generator matrix for C.

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

↳ RS codes are strongly explicit (Ex. 6.9)

$$i \rightarrow \begin{pmatrix} & \overset{j}{(\alpha_i)^j} & \end{pmatrix}$$

compute in poly(log q) time.

(Next) Big Goal: Can we get (strongly) explicit construction of codes with poly time decoding + encoding that achieves BSC_p capacity? (nearlinear time)

Recent(ish) Polar codes

(Q') Above with $R > 0$, $p > 0$? (Ex 6.13 in book)

Hamming vs. Shannon (qualitative)

Hamming	Shannon
Focus on codewords	Directly deals w/ encoding/decoding
Explicit codes	Not explicit at all!
R vs. δ	R vs "error parameter"
Worst-case error	memoryless stochastic channels

Obs: If a code C can handle $(p+\varepsilon)$-frac of worst-case errors $\Rightarrow$ can use C for reliable communication over BSC_p

$\Rightarrow$ By Chernoff Prob of $> (p+\varepsilon)n$ error is $\leq e^{-\varepsilon^2 n/2}$

Converse: If you can achieve exp. small decoding error prob over BSC_p with code C $\Rightarrow$ C has relative dist $\Omega(1)$ (Ex 6.5)

Quantitative Hamming vs. Shannon (Large q)

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

$\Rightarrow p_{Ham} \leq \frac{1-R}{2}$ frac. of (worst-case) errors

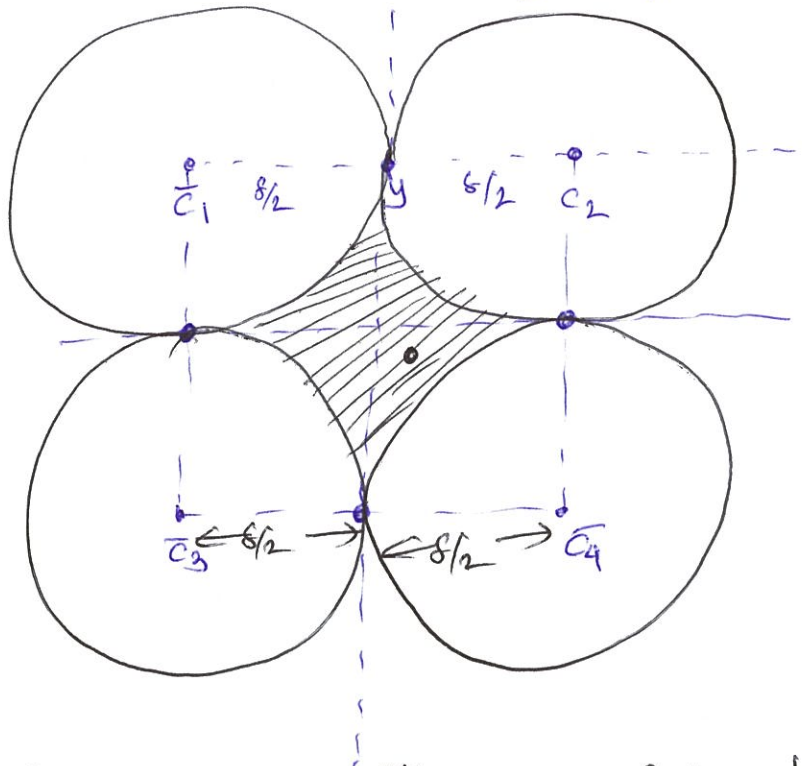
Shannon: qSC_p: capacity $R = 1-H_q(p)$

It can be shown (Prop 3.3.4) $1-p-\varepsilon \leq 1-H_q(p) \leq 1-p$, $q \geq 2^{\Omega(1/\varepsilon)}$

$\Rightarrow p_{Shannon} \geq 1-R-\varepsilon$

$\Rightarrow$ can correct up to twice as many errors in Shannon's setting.

Let revisit the $< \frac{\delta}{2}$ argument.



Any y on ¦ is a bad example.

In ▨ exception -¦-, every received word has a unique closest by codeword!

BUT we're not decoding those!

Q: How much of ▨ space relative to Σ^n space!

A: Pretty much ALL of it!

(Take as a given: the $\frac{c}{4}$ -¦- is a negligible frac of points)

$\boxed{q=2}$ Volume of all Hamming balls

$$\le 2^k \cdot Vol_2\left(\frac{\delta n}{2}, n\right)$$

$$\le 2^k \cdot 2^{H(\frac{\delta}{2})n} = 2^{Rn} \cdot 2^{H(\frac{\delta}{2})n}$$

$$= 2^{n(R+H(\frac{\delta}{2}))}$$

$\Rightarrow$ empty space ratio $\ge \dfrac{2^n - 2^{n(R+H(\frac{\delta}{2}))}}{2^n}$

By Hamming bound:

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

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

$$= 1 - \frac{2^{n(R+H(\frac{\delta}{2}))}}{2^n} = 1 - 2^{n(R+H(\frac{\delta}{2})-1)}$$

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

$$= 1 - 2^{-\gamma n} \longrightarrow 1 \quad \blacksquare$$

as $n \to \infty$