Apr 5 — 1 min checkin

REMINDERS

(•) HW 4 due by 11:59pm TONIGHT
(•) HW 5 out by 11:59pm tonight

RECAP

(•) Hamming (worst case errors) vs Shannon (memoryless stochastic errors)
(•) If C can correct $(p+r)$-fraction of worst-case errors
$\Rightarrow$ C has reliable communication ($2^{-\Omega(n)}$ dec. error prob) over BSC_p

Plan for today (•) Quantitative Hamming vs Shannon
(•) List decoding

Quantitative Hamming vs. Shannon

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

$\Rightarrow \leq \frac{1-R}{2}$ frac of errors $\left(\leq \frac{1}{2}\right)$

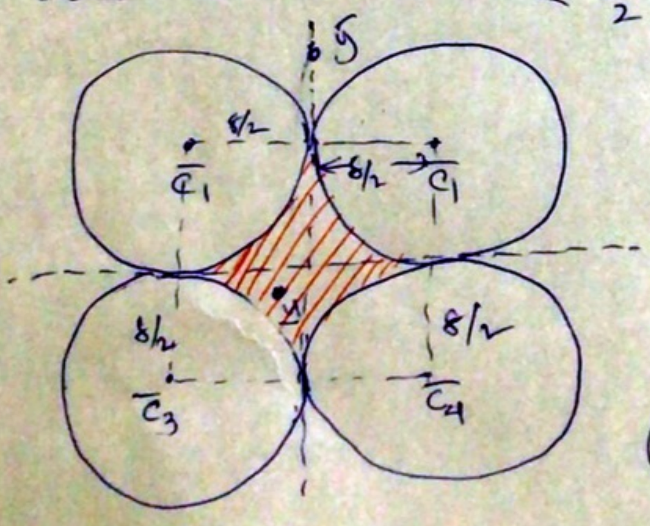
Shannon: qSC_p cap: $R \leq 1 - H_q(p)$

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

$\Rightarrow R \leq 1-p-\varepsilon \equiv p \leq 1-R-\varepsilon$ — can correct upto twice as many errors in Shannon's setting

---

Let's revisit the $< \frac{\delta}{2}$ frac of errors result.



Any $\bar{y}$ on - - - is a bad case.
But consider any y in [shaded region] but not - - -, such $\bar{y}$ have a unique closest codeword
$\Rightarrow$ for some error patterns with $> \frac{\delta}{2}$ frac. of errors we can recover the transmitted codeword!
$\Rightarrow$ But in the Hamming setting we are not even trying to decode from these!

Q: ~~How much~~ of the entire space is $\setminus$ -|- points?
What fraction

A: 1 as $n \to \infty$

Take as given that -|- is a small fraction $\to 0$ as $n \to \infty$

$\boxed{q=2}$

$\to$ Volume of all Hamming balls

$k = Rn$

$$\leq 2^k \cdot \mathrm{Vol}_2\left(\frac{\delta n}{2}, n\right)$$

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

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

$\Rightarrow$ total empty space

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

frac ______

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

Recall: Hamming bound

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

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

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

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

$$= 1 - 2^{-\gamma n} \xrightarrow[\text{as } n \to \infty]{} 1$$ ■

We ~~not~~ know if

$\swarrow$ Shannon's setup: relax this

(1) Deal w/ worst-case errors

AND

(2) Always have to output the transmitted codeword

unique decoding

$\}\Rightarrow \leq \frac{\delta}{2}$ errors

$\nwarrow$ Relax this $\to$ list decoding

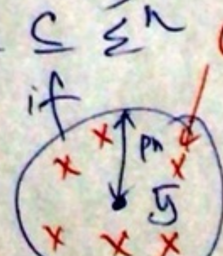
List decoding (Elias Wozencraft late '50s)

Def $0 \leq p \leq 1$, $L \geq 1$. We say a code $C \subseteq \Sigma^n$ is (p, L)-list decodable [(p,L)-l.d.] if

$$\forall \bar{y} \in \Sigma^n \quad |C \cap B(\bar{y}, pn)| \leq L$$

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

$\in C$



$\# \times \leq L$

<u>Algo version</u> Let C be (p, L)-l.d. Let $\bar{y} \in \Sigma^n$

→ output all $(\le L)$ $\bar{c} \in C$ s.t. $\Delta(\bar{y}, \bar{c}) \le pn$

Q: For what value of L is any code $(1, L)$-l.d.

L ↑ $|C|$

as $C \cap B \subseteq C$

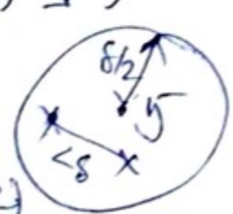
↳ <u>Poly time</u> list decoding algo, $\boxed{L \le poly(n)}$

<u>Q: If</u> C has rel. dist δ, C is $(< \frac{\delta}{2}, 1)$-l.d.

More generally (p, L)-l.d. C

→ transmit $\bar{c} \in C$ & say $\le pn$ ~~fault~~ errors (worst-case)

recd word → $\bar{y}$



⇒ $B(\bar{y}, pn) \ni \bar{c}$

$1 \le L$

→ What do you do with a list size > 1

(•) You ~~do not~~ have ~~any~~ side information about $\bar{c}$

(analogy: spell checker)

↳ use this extra information to disambiguate the list of size $\le L$

In principle $O(\log L)$ bits of information

↳ $O(\log n)$ if $L \le poly(n)$

↳ Extremely useful in complexity application

(•) You do <u>not</u> have any side information.

⇒ declare an error!

↳ For most error patterns list size is 1.

(•) For any code, random error patterns w/ $\le \delta - \varepsilon$ frac of errors, list size $= 1$ whp (Sec 7.5)