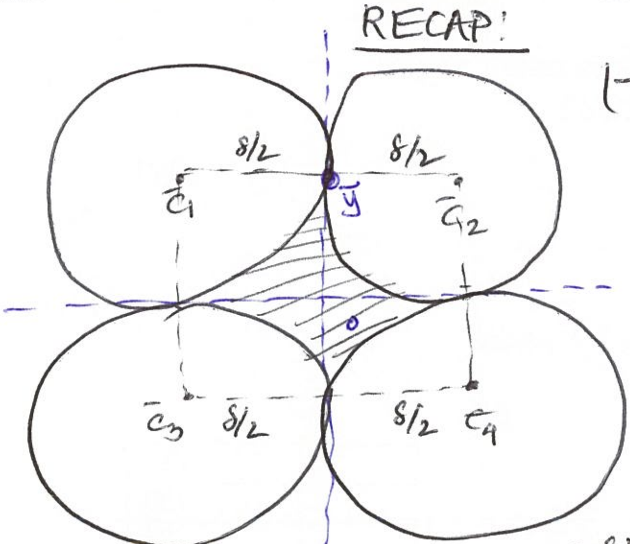
Mar 30

REMINDERS

(∘) Mini-project 2 pg. report due by 11:59pm TONIGHT
(∘) HW 4 out today
(∘) Please double check your proof reading assignment

RECAP:



(→) Every received word in ▨ region except those in ┼ have a UNIQUE closest by codeword BUT we give up on decoding these currently

(→) The ▨ region is pretty much the entire space as $n \to \infty$

(∘) (for large enough $q \geq 2^{\Omega(1/\varepsilon)}$) $\rho_{Ham} \leq \frac{1-R}{2}$, $\rho_{Shannon} \geq 1-R-\varepsilon$

TODAY

(∘) Proof readers: Samarth, Roshan
(∘) List Decoding

We know if

Shannon's setup: relax this?

(1) Deal with worst-case errors; AND
(2) Always need to output $\underline{\text{the}}$ transmitted codeword/message

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

unique decoding

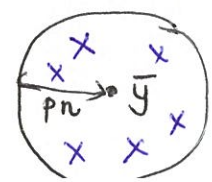
→ Next: relax this condition (list decoding)

LIST DECODING (Elias, Wozencraft late 50s)

~~Def~~ Def: $0 \leq \rho \leq 1$, $L \geq 1$. We say $C \subseteq \Sigma^n$ is (ρ, L)-list decodable [or (ρ, L)-l.d.] if

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

$= |\{\bar{c} \in C \mid \Delta(\bar{y}, \bar{c}) \leq \rho n\}| \leq L.$

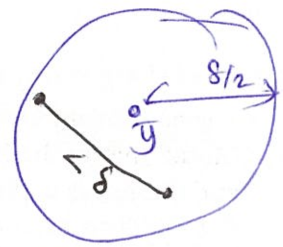


x: codeword
#x ≤ L

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

More generally, (p, L)-l.d. code $C \Rightarrow$ for any transmitted codeword if $< pn$ errors occur (& $\bar{y}$ is the recvd. word)
$\Rightarrow$ $B(\bar{y}, pn)$ has $\leq L$ codewords INCLUDING the transmitted codeword.

if not



Algo Q: ~~Given~~ Let C ~~B~~ be a (p, L) l.d. code.
Given $\bar{y} \in \Sigma^n$, output $C \cap B(\bar{y}, pn)$ ← list decoding algo

$\Rightarrow$ for poly list decoding algo, $L \leq \text{poly}(n)$

WANT: L to be poly(n).

What to do if list size > 1?

(0) You have no extra (side) information
↳ Declare an error?
↳ Can handle more error patterns
random errors (total frac of errors $\leq \delta - \varepsilon$) whp list size $= 1$. (See 7.5)
large alphabet size $q \geq 2^{\Omega(1/\varepsilon)}$

(1) If $\exists$ side information (analogy: spell checker) $\Rightarrow$ use it to disambiguate the list of L codewords. In principle $O(\log L)$ extra bits of information.
↳ $O(\log n)$ bits if $L \leq \text{poly}(n)$
↳ VERY USEFUL in complexity application.

Q1: Can we correct $> \frac{\delta}{2}$ frac of errors with poly(n) list size?

Q2: What is the optimal tradeoff between R & p for $(p, \text{poly}(n))$-l.d. code?

A1: Yes! For all codes! (Johnson bound)

THM (Johnson bound) $q \geq 2$, $C \subseteq [q]^n$ with dist d

If $p \leq J_q\left(\frac{d}{n}\right) \Rightarrow C$ is $(p, \underbrace{qdn}_{\text{poly}(n)})$-l.d.

$\frac{d}{n} = \delta$

poly(n) as long as q is poly(n)

$$J_q(X) = \left(1 - \frac{1}{q}\right)\left(1 - \sqrt{1 - \frac{qX}{q-1}}\right)$$

Lemma 1: $\forall\ q \geq 2,\ 0 \leq X \leq 1 - \frac{1}{q}$

(pf in book) $J_q(X) \geq 1 - \sqrt{1-X} > \frac{X}{2}$

$\Rightarrow J_q(\delta) > \frac{\delta}{2}$

$\Rightarrow$ Any $(n, k, d)_q$ code is $\left(\frac{e}{n}, qdn\right)$ l.d $\quad e \leq n - \sqrt{n(n-d)}$, $\ n(n-d) = n^2\left(1 - \frac{d}{n}\right)$

$\frac{e}{n} \leq 1 - \sqrt{1-\delta}$

Assume C is MDS $\quad \delta = 1 - R$

$\xrightarrow{\text{Johnson bound}} \quad p \leq 1 - \sqrt{1-(1-R)} = 1 - \sqrt{R}$

Q: Is Johnson bound tight?

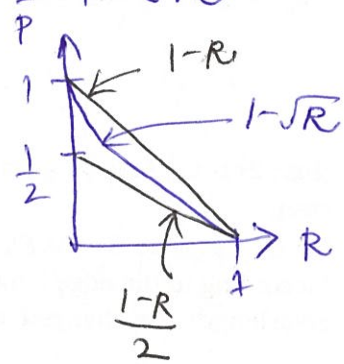
$p \leq 1 - \sqrt{1-\delta}$

YES! $\exists$ code with rel dist δ s.t.

$p > 1 - \sqrt{1-\delta} \Rightarrow$ super-poly many codewords?

NO: Random codes do better!

(Explicit)



Pf of Johnson bound ($q = 2$)

Proof technique: Double counting (to prove some inequality)

1. Come up w/ some quantity S
2. Show by (approx) counting that

   (i) $S \leq U$ (ii) $S \geq L$

   $\Rightarrow U \geq L$
3. (Somehow) use this to prove the required inequality.