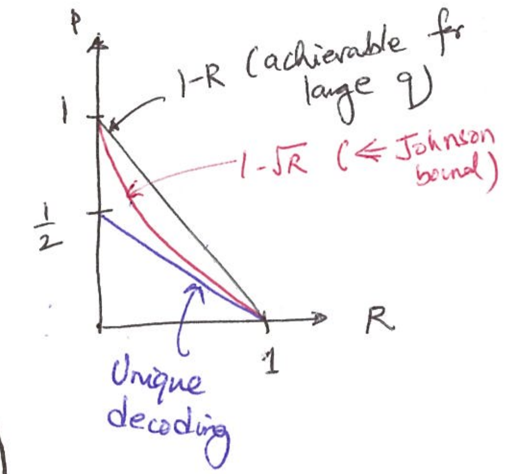
April 2, 2019

REMINDERS / ANNOUNCEMENTS

(•) Mini-project report due by 11:59pm tonight.
  → Every group submits (the same report) individually
  → No report $\Rightarrow$ 0 on video.

(•) HW 3 grading will be delayed.
  → My goal of the next week is to grade the reports first.

RECAP:



Def: A code $C \subseteq [q]^n$ is (p, L)-list decodable if $\forall\ \bar{y} \in [q]^n$,

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

Johnson bound: Every MDS code of rate R is $(1-\sqrt{R}, \text{poly}(n))$-l.d.

$\boxed{\begin{array}{l} \text{Johnson bound: } p \leq J_q(\frac{d}{n}) \\ J_q(\delta) = \left(1-\frac{1}{q}\right)\left(1-\sqrt{1-\frac{q\delta}{q-1}}\right) \\ \Rightarrow (p, qdn)\text{-l.d.} \end{array}}$

List decoding capacity:
$q \geq 2$, $0 < p < 1 - \frac{1}{q}$. Follow is true for large enough n:

(i) Let $L \geq 1$, $\exists$ (p, L)-l.d with rate

$$R \leq 1 - H_q(p) - \frac{1}{L}$$

Proved this last time

(ii) For every (p, L)-l.d. of rate $1 - H_q(p) + \varepsilon \Rightarrow L \geq q^{\Omega(\varepsilon n)}$.

TODAY (Proof reader: Dennis)

(•) Prove part (ii) of list decoding capacity result.

(•) More R v δ upperbounds → Elias-Bassalygo bound
  MRRW bound.

Done with combinatorial results.

(•) Code concatenation

Let $C \subseteq [q]^n$ be a (p,L)-l.d. code of rate $1-H_q(p)+\varepsilon$

$$\Rightarrow L \geq q^{\Omega(\varepsilon n)}$$

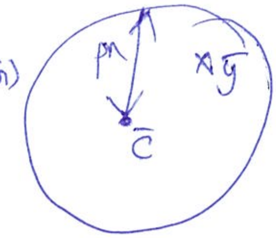
Pf: Fix $C \subseteq [q]^n$ with rate $R = 1-H_q(p)+\varepsilon$

Show $\exists\, \bar{y} \in [q]^n$ s.t. $|B(\bar{y}, pn) \cap C| \geq q^{\Omega(\varepsilon n)}$

→ Pick $\bar{y} \in [q]^n$ at random. (we'll use prob. method)

Fix $\bar{c} \in C$, $\Pr[\Delta(\bar{y},\bar{c}) \leq pn]$

$$= \frac{Vol_q(pn,n)}{q^n} \geq \frac{q^{H_q(p)n - o(n)}}{q^n}$$



$$= q^{-n(1-H_q(p))-o(n)}$$

$$\mathop{\mathbb{E}}_{\bar{y}}[|B(\bar{y},pn)\cap C|]$$

$$= \mathop{\mathbb{E}}_{\bar{y}} \sum_{\bar{c}\in C}\left(\mathbb{1}_{\Delta(\bar{y},\bar{c})\leq pn}\right)$$

linearity of exp $\Rightarrow$

$$= \sum_{\bar{c}\in C} \mathop{\mathbb{E}}_{y}\left(\mathbb{1}_{\Delta(\bar{y},\bar{c})\leq pn}\right) = \sum_{\bar{c}\in C} \underbrace{\Pr[\Delta(\bar{y},\bar{c})\leq pn]}_{\geq}$$

$$\geq \sum_{\bar{c}\in C} q^{-n(1-H_q(p))-o(n)} = q^{Rn}\, q^{-n(1-H_q(p))-o(n)}$$

$$= q^{n(1-H_q(p)+\varepsilon-(1-H_q(p)))-o(n)}$$

$$= q^{\varepsilon n - o(n)} \geq q^{\Omega(\varepsilon n)} \text{ as } \frac{o(n)}{n} \xrightarrow[n\to\infty]{} 0.$$

$\Rightarrow \exists\, \bar{y}$ s.t. $|C \cap B(\bar{y}, pn)| \geq q^{\Omega(\varepsilon n)}$ ∎

Cor: $\exists\, \bar{y} \in [q]^n$ s.t. $|C \cap B(\bar{y},pn)| \geq |C| \cdot \frac{Vol_q(pn,n)}{q^n}$

List decoding "capacity": $1-H_q(p)$

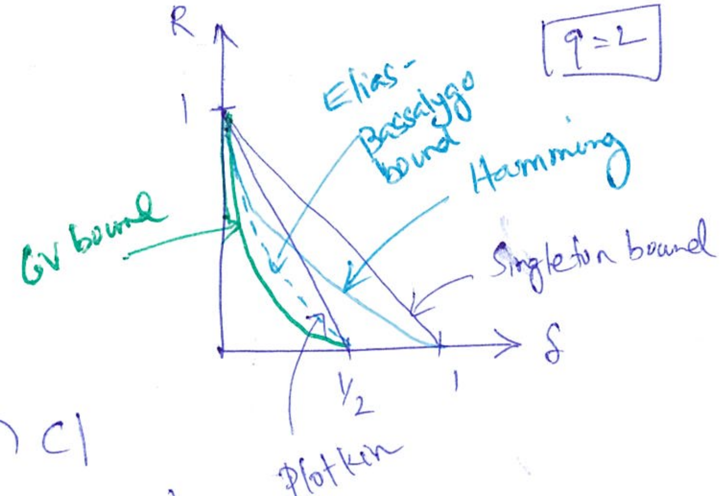
Q1: Explicit code that achieves LD capacity?

Q2: ______ + efficient encoding + list decoding alg

Q3: Above but $p = 1-\sqrt{R}$? ← RS codes

Ans: Yes to all!

Back to R vs δ.



Elias - Bassalygo bound:

q-ary code of rate R, rel. dist δ

$$R \leq 1 - H_q(J_q(\delta)) + o(1)$$

$$e = J_q(\delta)n - 1$$

$$\Rightarrow \forall \bar{y} \in [q]^n, \ |B(\bar{y}, e) \cap C| \leq qdn$$

$\uparrow$ Johnson bound.

But by ~~cor~~ COR

$$\exists \bar{y}^* \text{ s.t } |B(\bar{y}^*, e), C| \geq \frac{|C| \, Vol_q(e,n)}{q^n}$$

$$\Rightarrow |C| \frac{Vol_q(e,n)}{q^n} \leq qnd = q^{o(n)}$$

$$\Rightarrow |C| = q^k \leq \frac{q^n \cdot q^{o(n)}}{Vol_q(e,n)} \leq \frac{q^{n+o(n)}}{q^{H_q(J_q(\delta))n - o(n)}}$$

$$\Rightarrow q^{Rn} \leq q^{n(1 - H_q(J_q(\delta))) + o(n)}$$

$$\Rightarrow R \leq 1 - H_q(J_q(\delta)) + o(1) \quad \blacksquare$$

McEliece, Rodemich, Rumsey, Welch bound (MRRW bound)

$(q=2)$

$\delta = \frac{1}{2} - \varepsilon$: GV $\rightarrow$ $R_{GV} \geq \Omega(\varepsilon^2)$

$(\varepsilon \to 0)$ MRRW $\rightarrow$ $R_{MRRW} \leq O(\varepsilon^2 \log \frac{1}{\varepsilon})$

RECAP:

$(q=2)$

Shannon	Hamming	
	Unique	List
BSC_p		
$1-H(p)$ is cap	$R \geq 1-H(p)$ $R \leq$ MRRW	$1-H(p)$ is cap
Explicit codes at cap?	Explicit asymptotically good code? $R>0, \delta>0$	Explicit codes at cap?

Efficient decoding algos?

STILL OPEN!

(i) R vs optimal tradeoff $(q=2)$ ... $q<49$

(ii) Explicit codes on GV bound $(q=2)$ $q<49$.

① Decode RS $\frac{1-R}{2}$ errors in poly(n) ti[me]

② Explicit binary asymptotically good codes?

③ After ②, efficiently decode $>$ [...] frac. of errors.

Q: Is there an explicit binary code w/ $R>0$, $\delta>0$

Consider RS code over $\mathbb{F}_{2^s}$

$R=\frac{1}{2}$

	R	δ
Hamming	$1-O\left(\frac{\log n}{n}\right)$	$\Theta\left(\frac{1}{n}\right)$
Hadamard	$O\left(\frac{\log n}{n}\right)$	$\frac{1}{2}$
"RS"	$\frac{1}{2}$	$\frac{1}{2s}=\frac{1}{2\log n}$

Think of each element in $\mathbb{F}_{2^s}$ as $\{0,1\}^s$ $\Rightarrow$ $(ns, ks, n-k+1)_2$ ← this is tight since $\alpha\neq\beta\in\mathbb{F}_{2^s}$ $\Delta(\mathrm{bin}(\alpha),\mathrm{bin}(\beta))\geq 1$

$n=2^s$

Can fix the above if $c': \mathbb{F}_{2^s}\to\{0,1\}^{2s}$ s.t. $\Delta(c'(\alpha),c'(\beta))\geq\Omega(s)$ for $\alpha\neq\beta\in\mathbb{F}_{2^s}$

asymptotically good code.

Code Concatenation:

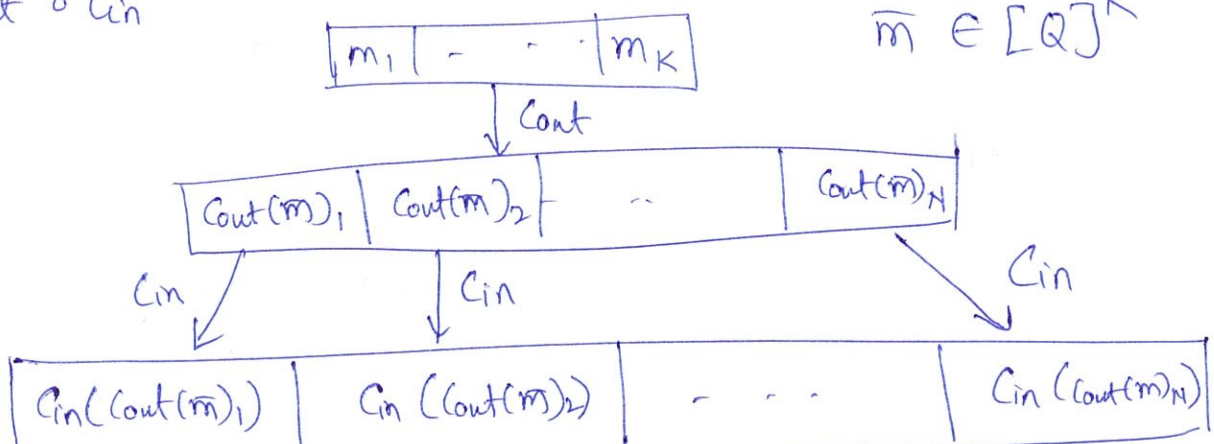
$Q=q^k$

$C_{out}: [Q]^K \to [Q]^N$ } outer code

$C_{in}: [q]^k \to [q]^n$ } inner code

$C_{out}\circ C_{in}$

$\bar{m}\in[Q]^K$



THM: If C_{out} is $(N,K,D)_{q^k}$ code, C_{in} is $(n,k,d)_q$ code

$C_{out}\circ C_{in}$ $(Nn, Kk, Dd)_q$ codes (Also linearity is preserved).

C_{out}: R, δ_{out}

C_{in}: r, δ_{in}

$\Rightarrow$ $C_{out}\circ C_{in}$: Rr, $\delta\geq\delta_{in}\cdot\delta_{out}$

($n, k \sim O(\log N)$)