Apr 6

REMINDERS

(1) HW 4 due by 11:59 pm TONIGHT

(2) HW 5 out by 11:59pm tonight

RECAP

(•) JOHNSON BOUND: Let $C \subseteq [q]^n$ have dist $d = \delta n$.

Iff $\rho \le J_q(\delta) \Rightarrow C$ is (ρ, qdn)-l.d.

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

(•) COROLLARY (of pf. of list decoding capacity)

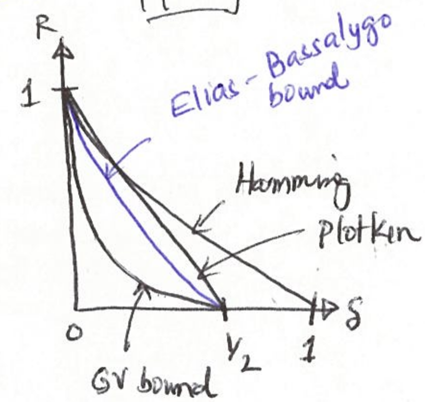
Let $C \subseteq [q]^n$ be a code. $\exists\ \bar{y}^* \in [q]^n$ s.t.

$$|B(\bar{y}^*, \rho n) \cap C| \ge |C| \cdot \frac{Vol_q(\rho n, n)}{q^n} \quad (1)$$

(•) Elias-Bassalygo bound

Any q-ary code of rel dist δ has $R \le 1 - H_q(J_q(\delta)) + o(1)$

$q=2$



TODAY:

(•) Pf readers: Sai Sriram, Abdullah

(•) Elias-Bassalygo bound pf + more on R vs δ

(•) Code concatenation

Let C be a code of rel. dist δ

$e = J_q(\delta)n - 1 \Rightarrow \rho = \frac{e}{n} < J_q(\delta)$.

By the Johnson bound, $\forall\ \bar{y} \in [q]^n$ $|B(\bar{y}, e) \cap C| \le qdn$

from $\Rightarrow |B(\bar{y}^*, e) \cap C| \le qdn$

from (1) $\Rightarrow qdn \ge |C| \cdot \frac{Vol_q(\rho n, n)}{q^n}$

$$\Rightarrow q^{Rn} = |C| \le \frac{q^n \cdot (qdn)}{Vol_q(\rho n, n)} \le \frac{q^n \cdot q^{o(n)}}{q^{H_q(\rho)n - o(n)}}$$

$$= q^{n + o(n) - H_q(\rho)n + o(n)}$$

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

$\Rightarrow R \le 1 - H_q(\rho) + o(1) \le 1 - H_q(J_q(\delta)) + o(1)$ ∎

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

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

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

RECAP:

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

STILL OPEN: (1) Optimal R vs δ tradeoff? $(q<49)$

(2) Explicit codes on GV bound? $(q<49)$

(1) Decode RS codes from $\frac{1-R}{2}$ errors? uniquely

(2) Explicit binary ~~asym~~ asymptotically good codes? ← $(q=2)$

(3) After (2), efficient decoding from >0 frac of errors?

	R	δ
Hamming	$1-O(\frac{\log n}{n})$	$\Theta(\frac{1}{n})$
Hadamard	$O(\frac{\log n}{n})$	$\frac{1}{2}$
RS codes with binary repr of $\mathbb{F}_{2^s}$	$\frac{1}{2}$	$\geq \frac{n/2}{ns} = \frac{1}{2s} = O(\frac{1}{\log n})$

Look back at explicit binary codes

$\frac{k}{n} = \frac{1}{2}$

$q = n = 2^s$
$\Rightarrow s = \log n$

Consider RS code over $\mathbb{F}_{2^s}$ $R = \frac{1}{2}$ $\delta = \frac{1}{2}$

$[n, k, n-k+1]_{2^s}$ RS code.

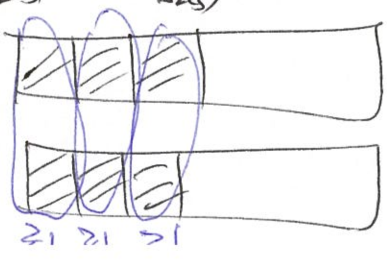
↳ Think of each element in $\mathbb{F}_{2^s}$ as in $\{0,1\}^s$ $\longrightarrow$ $(ns, ks, \geq n-k+1)_2$

$(\mathbb{F}_{2^s})^k \equiv \{0,1\}^{ks}$

$\alpha \neq \beta \in \mathbb{F}_{2^s}$

$\Delta(bin(\alpha), bin(\beta)) \geq 1$

$bin(\alpha), bin(\beta) \in \{0,1\}^s$



What if we had access $C' : \mathbb{F}_{2^s} \to \{0,1\}^{2^s}$ s.t.

$\forall \alpha, \beta \in \mathbb{F}_{2^s}, \quad \Delta(C'(\alpha), C'(\beta)) \geq \Omega(S)$

Code Concatenation

$C_{out} : [Q]^K \to [Q]^N \qquad Q = q^k$

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

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

$\boxed{m_1 \mid \cdots \mid m_K} \quad \bar{m} \in [Q]^K$

$\downarrow C_{out}$

$\in [q^k]$

$\boxed{C_{out}(\bar{m})_1 \mid \cdots \mid C_{out}(\bar{m})_i \mid \cdots \mid C_{out}(m)_N}$

$\downarrow C_{in} \qquad \downarrow C_{in} \qquad \downarrow C_{in}$

$\boxed{C_{in}((C_{out}(\bar{m}))_1) \mid \cdots \mid C_{in}((C_{out}(\bar{m}))_i) \cdots \mid C_{in}((C_{out}(\bar{m}))_N)}$

$\in [q]^n$

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

$\Rightarrow C_{out} \circ C_{in}$ $(Nn, Kk, Dd)_q$-code (linearity is preserved)

$C_{out} : R, \delta_{out} \qquad C_{in} : r, \delta_{in} \Rightarrow C_{out} \circ C_{in} : Rr = \mathcal{R}$

$\delta = \delta_{out} \cdot \delta_{in}$

If we get $R > 0, \ \delta_{out} > 0$

$r > 0, \ \delta_{in} > 0 \qquad \Rightarrow \mathcal{R} > 0, \ \delta > 0$

RS