| Apr12 |

1 min checkin

REMINDERS

(•) HW 5 due 11:59pm tonight

(•) HW 6 (last HW!!) out by 11:59pm tonight

↳ If you plan to drop HW 5+6, please do NOT submit

(•) Video due in 4.5 weeks (11:59pm, Sun, May 14)

↳ Please take my comments + grading rubric of report into account!

RECAP

(•) Johnson bound: Let $C \subseteq [q]^n$ have $d = \delta n$.

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

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

(•) COROLLARY (of proof of list decoding capacity results)

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

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

Plan for today (•) Elias-Bassalygo bound (•) More on R vs. δ & q

(•) (If there is time) code concatenation

List decoding Capacity $\equiv p \approx 1 - R - \varepsilon$, $q \ge 2^{\Omega(1/\varepsilon)}$

$1 - H_q(p) \approx 1 - p - \varepsilon$ if $q \ge 2^{\Omega(1/\varepsilon)}$; $1 - H_q(p) = R$, $\forall q$

Q1) Explicit codes that achieve l.d. capacity? $p \approx 1 - R - \varepsilon$

Q2) ______ w/ efficient encoding + decoding

Q3) Above (Q2) with $p = 1 - \sqrt{R}$? Yes. (RS)

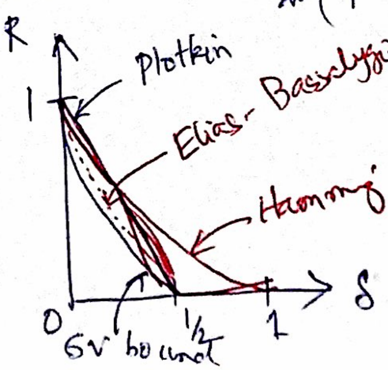
(As of last week $\exists$ RS codes that are $(1 - R - \varepsilon, O(\frac{1}{\varepsilon}))$ l.d.)

Back to R vs δ

Elias-Bassalygo bound

Any q-ary code of rate R & rel-dist δ

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



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

Pf: $e = J_q(\delta)n - 1 \Rightarrow p = \frac{e}{n} < J_q(\delta)$

Let C be a code of rel. dist. δ

By the Johnson bound $\Rightarrow C$ is (p, qdn)-l.d.

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

$\Rightarrow$ for $\bar{y}^*$ as in (1), $\quad |B(\bar{y}^*, e) \cap C| \leq qdn$

Otoh by Cor. $|B(\bar{y}^*, e) \cap C| \geq |C| \cdot \frac{Vol_q(pn, n)}{q^n}$

$$\Rightarrow qdn \geq |C| \cdot \frac{Vol_q(pn, n)}{q^n}$$

$$\Rightarrow |C| \leq \frac{q^n}{Vol_q(pn, n)} \cdot (qdn)$$

$$\Rightarrow q^{Rn} \leq \frac{q^n}{Vol_q(pn, n)} \cdot (qdn)$$

$$\leq \frac{q^n}{q^{H_q(p)n - o(n)}} \cdot q^{o(n)}$$

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

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

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

$$\Rightarrow R\cancel{n} \leq \cancel{n}(1 - H_q(p) + o(1))$$

$$< 1 - H_q(J_q(\delta)) + o(1) \quad \blacksquare$$

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

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

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

Recap:

	Shannon	Hamming		$q=2$
	BSC_p	Unique	List	
	Cap: $1-H(p)$	$R \geq 1-H(\delta)$ $R \leq MRRW$	Cap: $1-H(p)$	
	Explicit codes on capacity?	Explicit asymptotically good codes $R>0, \delta>0$	Explicit codes on capacity?	

Still open! (1) Optimal R vs δ tradeoff / ($q<49$)
Is GV bound optimal ($q \geq 49$ Algebraic Geometric codes)

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

(i) Uniquely decode RS codes of rate R from $\frac{1-R}{2}$ frac. of errors in poly time?

(ii) Explicit binary asymptotically good codes? ←

(iii) Once (ii) is done, 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 + binary em	$\frac{1}{2}$	$\Theta(\frac{1}{\log n})$

Look back at explicit binary codes (Goal: $R>0$, $\delta>0$)

$q = 2^s$

any element in $\mathbb{F}_q$ as $\{0,1\}^s$

$[n, k, n-k+1]_{q=2^s}$ $\quad q = 2^s = n$ $(\geq n)$

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

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

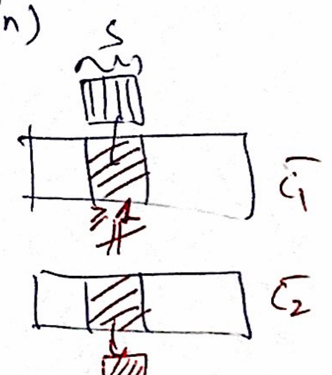
↳ replace each $\alpha \in \mathbb{F}_{2^s} \rightarrow bin(\alpha) \in \{0,1\}^s$

$(ns, ks, n-k+1)_2$

$\uparrow$

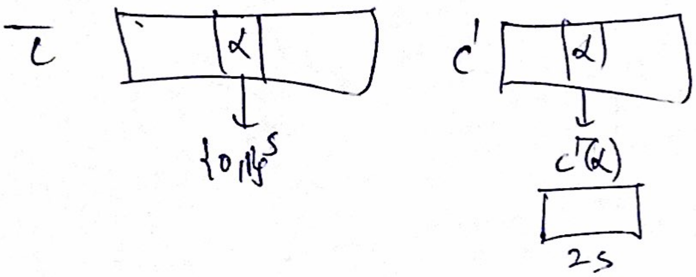
$(\mathbb{F}_{2^s})^k \equiv \{0,1\}^{ks}$ $\Rightarrow R_{new} = \frac{ks}{ns} = \frac{k}{n} = \frac{1}{2}$

$\delta_{new} \geq \frac{n-k+1}{ns} \geq \frac{n/2}{ns} = \frac{1}{2s} = \Theta(\frac{1}{\log n})$



Q: What if we had access to $C' : \mathbb{F}_{2^s} \to \{0,1\}^{2s}$

s.t. $\forall\ \alpha \neq \beta \in \mathbb{F}_{2^s}$ $\quad \Delta(C'(\alpha), C'(\beta)) \geq \Omega(s)$



$\to (2ns, ks, ?)$