March 1

1 min checkin

Please turn ON your camera If you can

REMINDERS

(1) Video topic due by 11:59 pm TONIGHT!

↳ If your group doesn't submit the form then EVERYONE in the group gets a 0 in the rest of the project.

→ Only ~~6~~ 11 groups have submitted by ~~11pm on Tue~~ 4pm today

(2) HW 2 out by tonight

RECAP

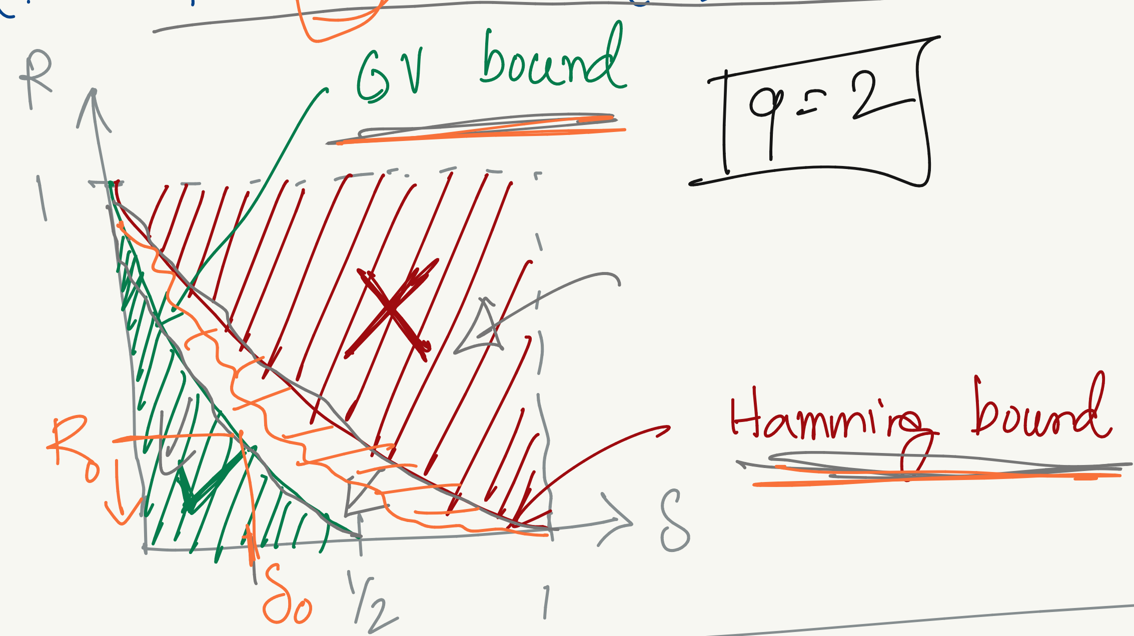
(•) Volume of a Hamming ball : $Vol_q(r,n) = |\{\bar{y} \in [q]^n \mid \Delta(\bar{y},\bar{x}) \le r\}|$

(•) $\boxed{q^{H_q(p)n - o(n)} \le Vol_q(pn,n) \le q^{H_q(p)\cdot n}}$ $p \le 1 - \frac{1}{q}$

(•) GV bound: $R \ge 1 - H_q(\delta) - \varepsilon$ (linear)

(•) Hamming bound: $R \le 1 - H_q\left(\frac{\delta}{2}\right) + o(1)$

Big Q! optimal tradeoff b/w R and δ?



Plan for today

(•) Prove GV bound

↳ We'll use probabilistic arguments today!

Gilbert-Varshamov (GV) bound

THM: Let $q \geq 2$, $0 \leq \delta \leq 1 - \frac{1}{q}$, $0 \leq \varepsilon \leq 1 - H_q(\delta)$ $\to 0$

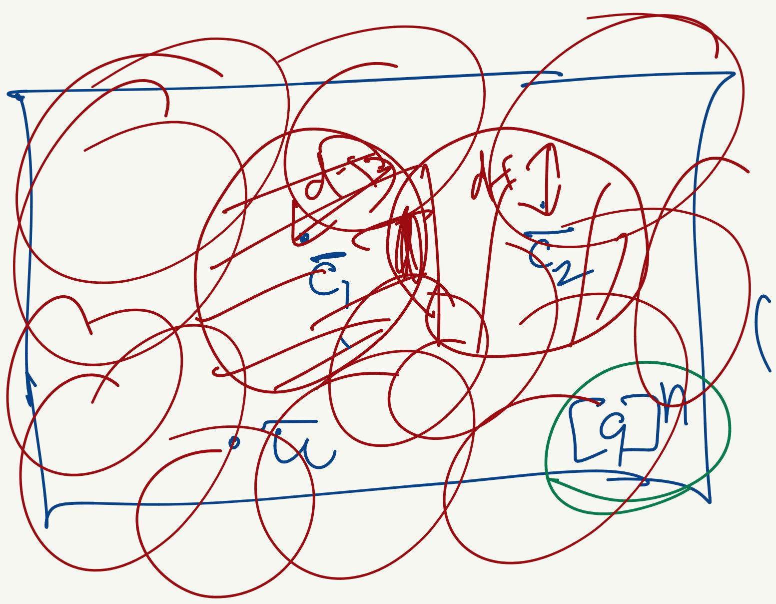
$\exists$ a (linear) code with rel. dist. δ and rate $R \geq 1 - H_q(\delta) - \varepsilon$

2 proofs: $\to$ Greedy construction $(\varepsilon = 0)$ $\to$ not necessarily a linear code [Gilbert]

$\to$ Randomized construction (linear codes) [Varshamov]

Q: How would you constr' a code with given distance $d = \delta n$? Hint: Greedy algo $\leftarrow$ not nec. efficient

Greedy construction



Algo

(1) $C \Leftarrow \phi$

(2) While $\bar{u} \in [q]^n$ s.t. $\boxed{\Delta(\bar{u}, \bar{c}) \geq d \ \forall\, \bar{c} \in C}$

Add $\bar{u}$ to C

(3) Return C $\leftarrow$ need not be linear

Claim 1: Algo terminates [Loop (2) runs at most q^n time]

Claim 2: C returned by Algo has dist $\geq d$ (by construction or algo def.)

Proposition: $$\boxed{|C| \geq q^{n(1-H_q(\delta))}}$$

$$k = \dim(C) \geq n(1-H_q(\delta))$$

$$\equiv \quad R \geq 1 - H_q(\delta)$$

Pf: As the algo terminates

$$\bigcup_{\bar{c} \in C} B(\bar{c}, d-1) = [q]^n$$

(if not then $\exists$ a $\bar{u}$ that you can add to C)

$$\Rightarrow \left| \bigcup_{\bar{c} \in C} B(\bar{c}, d-1) \right| = q^n$$

$$\leq \sum_{\bar{c} \in C} |B(\bar{c}, d-1)|$$

$$\left| \bigcup_{i=1}^{m} A_i \right| \leq \sum_{i=1}^{m} |A_i|$$

$$\Rightarrow q^n \leq \sum_{\bar{c} \in C} |B(\bar{c}, d-1)|$$

$$= \sum_{\bar{c} \in C} Vol_q(d-1, n)$$

$$\leq \sum_{\bar{c} \in C} Vol_q(\cancel{d}\ \delta n, n)$$

$$= |C| \cdot Vol_q(\delta n, n)$$

$$\leq |C| \cdot q^{H_q(\delta)n}$$

$$\Rightarrow q^n \leq |C| \cdot q^{H_q(\delta)n}$$

$$\Rightarrow |C| \geq \frac{q^n}{q^{H_q(\delta)n}}$$

$$= q^{n(1-H_q(\delta))}$$

$\blacksquare$

Varshamov's construction

Linear codes with rel. dist δ, $R \geq 1 - H_q(\delta) - \varepsilon$ $\quad \forall \varepsilon \geq 0$ $\quad \varepsilon > 0$

Probabilistic method

$\Pr$[a random linear code of rate $\geq 1 - H_q(\delta) - \varepsilon$ has rel dist $\geq \delta$] > 0

over distr. of random linear codes

$\Rightarrow \exists$ a $\forall$

$k = \lfloor (1 - H_q(\delta) - \varepsilon) n \rfloor$

What family of random linear codes

Pick any $G \in \mathbb{F}_q^{k \times n}$ uniformly at random

pick each entry independently uniformly at random for $\mathbb{F}_q$

$$k \left(\quad \right), \quad \longleftarrow n \longrightarrow$$

$\geq$ = fraction of $G \in \mathbb{F}_q^{k \times n}$ gives a linear code on GV bound.

$$\boxed{\Pr[\text{a random linear code of rate} \geq 1 - H_q(\delta) - \varepsilon \text{ has rel dist} \geq \delta] > 0}$$

new goal

$$\equiv \Pr[\text{a random linear code of rate } 1 - H_q(\delta) - \varepsilon \ \& \text{ dim } k \text{ has rel. dist} < \delta] < 1.$$

Probability lemmas

$\boxed{\text{read Sec 3.1, 3.2}}$

Lemma 1: Let $\bar{m} \in \mathbb{F}_q^k$ is non-zero. Let $G \in \mathbb{F}_q^{k \times n}$ is picked uniformly at random

$$\overset{\longleftarrow k \longrightarrow}{\begin{pmatrix} m \end{pmatrix}} \underset{\longleftarrow n \longrightarrow}{\begin{pmatrix} & G & \end{pmatrix}}\updownarrow k = \begin{pmatrix} \\ \\ \\ \end{pmatrix}\updownarrow n$$

$\bar{m} G \in \mathbb{F}_q^n$ is also uniformly random.

$$\bar{0} \cdot G = \begin{pmatrix} 0 \end{pmatrix} \text{ w.p. } 1$$

$$\bar{0} \cdot G = \bar{0}$$

Lemma 2: (Union Bound)

$$\Pr\left[\bigvee_{i=1}^{m} E_i\right] \leq \sum_{i=1}^{m} \Pr[E_i]$$