Mar 3 — 1-min checkin

REMINDERS

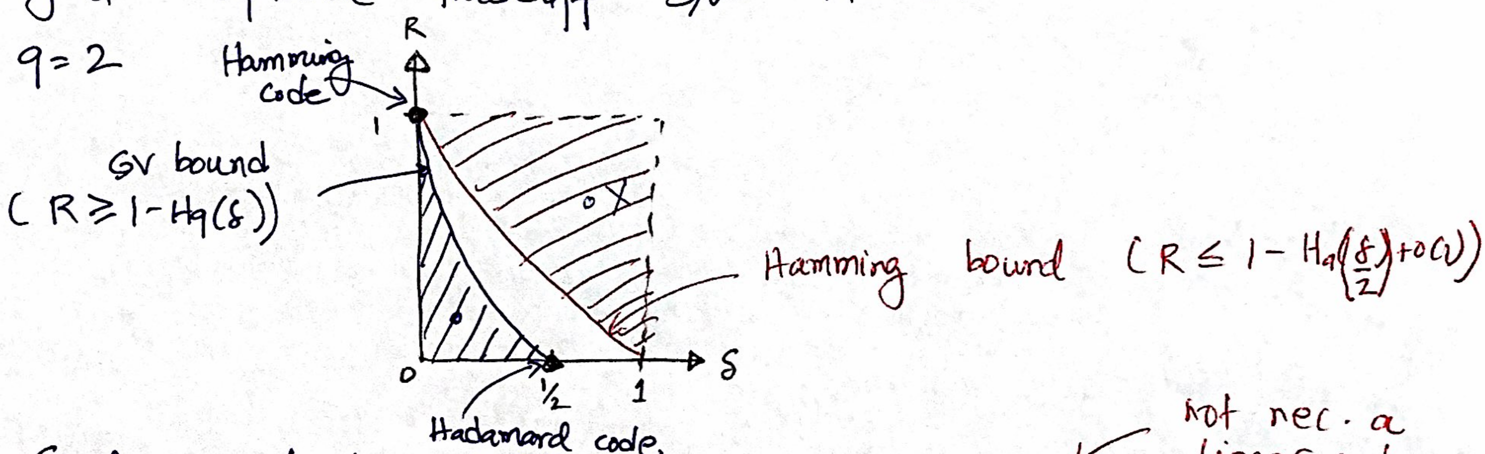
(1) Have responded to each group about their video topic choices
(2) HW 2 is out (due by 11:59pm on Wed)

ANNOUNCEMENT

(1) I'm out of town Mon & Wed
(2) I'll post lecture videos that y'all will need to see on Mon/Wed
(3) Ben will be on piazza 4:30-5pm on Mon / Wed to answer any questions
(4) Details on piazza by tomorrow (5) My OH on Monday is canceled
$\rightarrow$ Ben will have an extra OH Mon/Tue

RECAP

(•) Big Q : Optimal tradeoff b/w R & δ?
(•) $q=2$



(•) Greedy construction (Gilbert) $R \geq 1-H_q(\delta)$ — not nec. a linear code; $\delta \leq 1-\frac{1}{q}$
(•) $q^{H_q(p)n - o(n)} \leq Vol_q(pn, n) \leq q^{H_q(p)n}$ — Assuming $p \leq 1-\frac{1}{q}$
(•) Varshamov construction:
To prove $\rightarrow$ Pr [a random linear (k×n) code of rate $1-H_q(\delta)-\varepsilon$ has rel. dist $<\delta$] <1
dim $k = \lfloor (1-H_q(\delta)-\varepsilon)n \rfloor$
(•) Probability lemmas
Lemma 1: Let $\bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$. Let $G \in \mathbb{F}_q^{k \times n}$ be picked uniformly at random.
Then $\bar{m}G \in \mathbb{F}_q^n$ is uniformly random over $\mathbb{F}_q^n$
Union bound: $Pr[\bigvee_{i=1}^{m} E_i] \leq \sum_{i=1}^{m} Pr[E_i]$

Plan for today (•) Finish Varshamov construction/proof
(•) Singleton bound

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

Let $G \in \mathbb{F}_q^{k \times n}$ be a uniformly at random

We want to show (ultimately) that

$\forall \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\} \quad wt(\bar{m} G) \geq \delta n$ ($\equiv$ the code generated by G has dist $\geq \delta n$)

negate $\quad \exists \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\} \quad wt(\bar{m} G) < \delta n$

We need to show:

$$\boxed{\Pr_{G \in \mathbb{F}_q^{k \times n}} \left[\exists \bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\} \text{ s.t. } wt(\bar{m} G) < \delta n \right]} < 1$$

By union bound

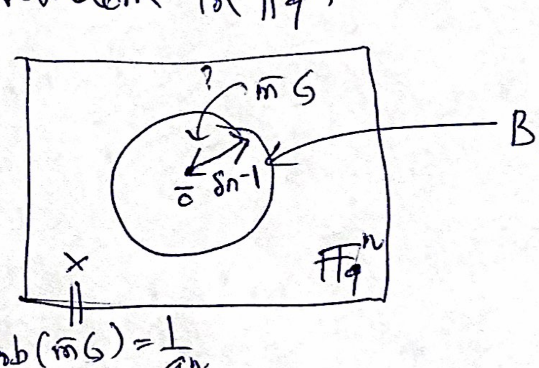
$$\leq \boxed{\sum_{\bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}} \underbrace{\Pr[wt(\bar{m} G) < \delta n]}_{< \frac{1}{q^k - 1}}} \quad (@) \cdots\cdots < 1$$

Fix $\bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}$

By Lemma 1, $\bar{m} G$ is uniformly random in $\mathbb{F}_q^n$

$\Pr[wt(\bar{m} G) < \delta n] =$

$\Pr[\text{random vector} \in \mathbb{F}_q^n \text{ falls in } B_0]$



$$= \frac{|B_0|}{q^n}$$

$$= \frac{Vol_q(\delta n - 1, n)}{q^n} \leq \frac{Vol_q(\delta n, n)}{q^n} \leq \frac{q^{H_q(\delta) \cdot n}}{q^n}$$

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

$$\Rightarrow (@) \leq \sum_{\bar{m} \in \mathbb{F}_q^k \setminus \{\bar{0}\}} q^{-n(1 - H_q(\delta))} \leq (q^k - 1)\, q^{-n(1 - H_q(\delta))}$$

$$< q^k q^{-n(1 - H_q(\delta))} \leq q^{(1 - H_q(\delta) - \varepsilon) n} \cdot q^{-n(1 - H_q(\delta))}$$

$$= q^{n(1 - H_q - \varepsilon - (1 - H_q(\delta)))} = q^{-\varepsilon n} \leq 1 \quad (<< 1 \text{ if } \varepsilon > 0)$$

$\Rightarrow (@) < 1 \quad \Rightarrow \exists G$ s.t. the code has rel. dist $\geq \delta$

Need to argue $\dim(G) = k \equiv G$ has full rank

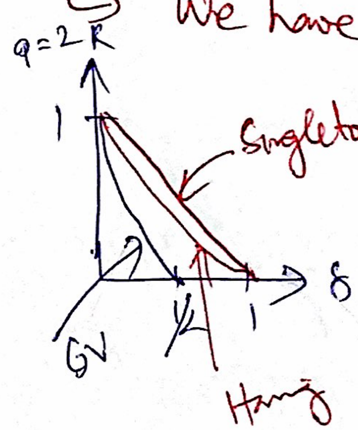
Option 1: Show whp random G has full rank $\approx 1 - \frac{1}{q^{n-k}}$

Option 2: for fixed $\delta > 0$, large enough n, $d = \delta n \geq 1$

Claim: If the code generated G has dist ≥ 1
$\Rightarrow G$ has full rank.

Singleton bound THM: Any $(n,k,d)_q$ code has
$d \leq n-k+1 \equiv k \leq n-d+1$
$\equiv R \leq 1-\delta+o(1)$

↳ We have argued this for linear codes

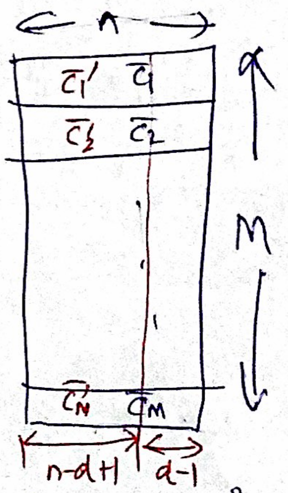


$\rightarrow q = 2$ $R \leq 1-\delta$ is not interesting

but as $q \to \infty$ (q depends on n)
then Singleton bound is tight
(RS code $d = n-k+1$)

Pf $k \leq n-d+1 \equiv q^k \leq q^{n-d+1}$

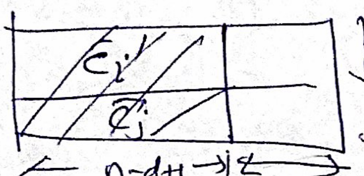
$|C| = \{\bar{c}_1, \dots, \bar{c}_M\}$ $M = q^k$



$\bar{c}_i'$ be $\bar{c}_i$ projected to the first $n-d+1$ posns

Claim: $\forall\, i \neq j$ $\bar{c}_i' \neq \bar{c}_j'$

Pf: If not $i \neq j$ $\bar{c}_i' = \bar{c}_j'$



$C' = \{\bar{c}_i' \mid c_i \in C\}$ $\Rightarrow \Delta(\bar{c}_i, \bar{c}_j) \leq d-1 \Rightarrow$ contradict C has dist d.

Claim $\Rightarrow$ $|C| = |C'| = M$

$M = |C'| \leq q^{n-d+1} \Rightarrow q^k \leq q^{n-d+1}$ ∎