5T08 LECTURE 04 2/19/08

Note Title 2/18/2008

TODAY: LIMITS ON RATES OF CODES

- Summary of what we know
- Hamming (Sphere-packing) Bound
- Plotkin Bound
- Elias Bound

Review: • $(n,k,d)_q$ code C maps $\overbrace{\Sigma^k \to \Sigma^n}^{x}$

with $\Delta(C) \geq d$, $|\Sigma| = q$

- $[\quad]$ $\Rightarrow$ linear code
- $q=2 \Rightarrow \exists$ code with $k \geq n - \log_2 Vol(n,d)$
- $R \triangleq \frac{k}{n}$; $\delta = \frac{d}{n}$;

$\Rightarrow \exists$ codes with $R \geq 1 - H(\delta)$

A simple bound [Singleton]:

Theorem: $\forall q \quad R + \delta \leq 1$

$$\Leftarrow \quad k + d \leq n + 1$$

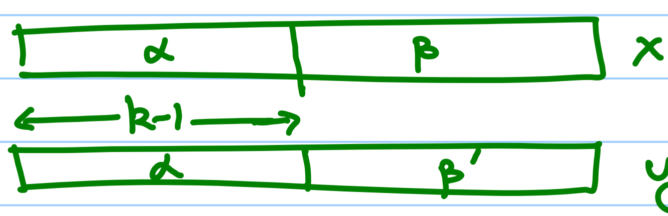
Proof: Project all codewords to first $k-1$ coord.

Projection function $\pi : \Sigma^n \to \Sigma^{k-1}$

Since # codewords $> |\Sigma|^{k-1}$

$\exists$ distinct codewords x, y s.t.

$$\pi(x) = \pi(y)$$



coordinates where they differ $\leq n - (k-1)$

$$\Rightarrow \quad d \leq n - k + 1.$$

Can we do better? For $q = 2$?

Recall

- Code of distance δ corrects $\delta/2$ errors
- $\Rightarrow$ $\exists$ codes correcting $\frac{\delta}{2}$ fraction of errors with rate $R \geq 1 - H(\delta)$
- Contrast with [Shannon] who guaranteed codes correcting $\frac{\delta}{2}$ fraction random, independent, errors with rate $R \geq 1 - H(\frac{\delta}{2})$.

  higher rate!

- [Shannon] Converse: $R \leq 1 - H(\frac{\delta}{2})$.

  [Hamming's]: Also proved $R \leq 1 - H(\frac{\delta}{2})$.

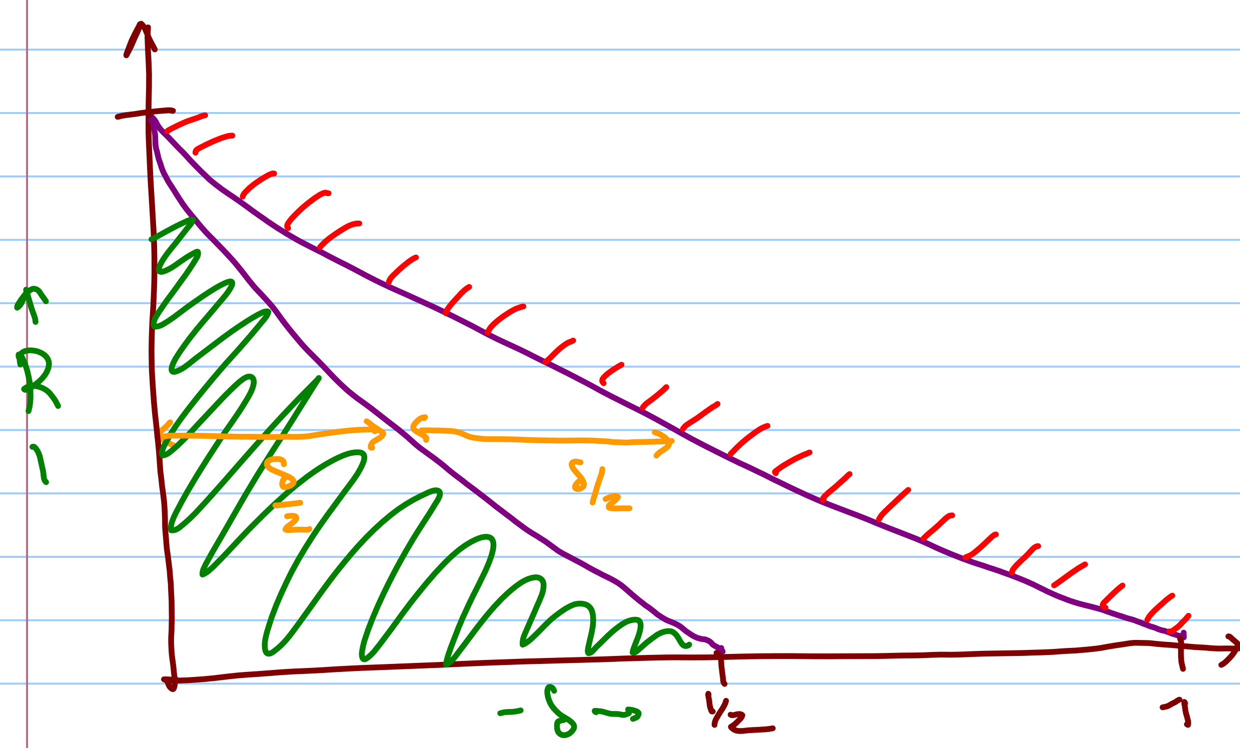
Hamming Bound

Idea: Balls of radius $\frac{d-1}{2}$ disjoint.

Conclusion: $2^k \cdot \mathrm{Vol}\left(n, \frac{d-1}{2}\right) \leq 2^n$

$$\Rightarrow \quad k + \log_2 \mathrm{Vol}\left(n, \frac{d-1}{2}\right) \leq n$$

$$\Rightarrow \quad R + H\left(\frac{\delta}{2}\right) \leq 1 \qquad [q=2]$$



Is the x-intercept right?

Can we really have binary codes with $\delta = .75$?

[Plotkin]'s Bound : $(q=2)$

$$R + 2\delta \leq 1$$

(i) $d > \frac{n}{2} \Rightarrow k \leq \log_2 n+1$

(ii) $\exists\, (n,k,d)$ code $\Rightarrow \exists\, (n-1, k-1, d)$ code

$\exists\, (n-1, k, d-1)$ code

Proof of (ii) :

- Say C is an $(n,k,d)_2$ code
- Let C_0 be all codewords ending with 0

C_1 " 1

- One of them satisfies $|C_i| \geq \frac{|C|}{2}$, say C_0

- Let $\tilde{C}_0$ be projection to last $n-1$ coord.

  Then $\tilde{C}_0$ has length $n-1$

  message length $\geq k-1$

  distance $\geq d$

  $\Rightarrow \exists\ (n-1, k-1, d)_2$ code

- Let $\tilde{C}$ be projection of C to last $n-1$ coords.

  $\tilde{C}$ has length $n-1$

  message length $\geq k$

  distance $\geq d-1$

$\boxtimes$ (ii)

Proof of (i): Hamming $\longrightarrow$ Euclid

Idea: • Map Σ to Euclidean space ...

s.t. Hamming distance maps to ℓ_2^2 distance

• Extend map to Σ^n & derive coding theory bounds from these.

Step 1: $\{0,1\} \longrightarrow \mathbb{R}^1$

$$0 \longrightarrow 1$$

$$1 \longrightarrow -1$$

Step 2: $\{0,1\}^n \longrightarrow \mathbb{R}^n$

$$x \longrightarrow \tilde{x}$$

$$\Delta(x,y) = d \implies \langle \tilde{x}, \tilde{y} \rangle = n - 2d$$

Now the coding theory :

- Suppose $C = \{x_1 \dots x_m\} \subseteq \{0,1\}^n$

  with $\Delta(x_i, x_j) > \frac{n}{2}$

- Euclidean version $\tilde{C} = \{\tilde{x}_1, \dots \tilde{x}_m\} \subseteq \mathbb{R}^n$

  with $\langle \tilde{x}_i, \tilde{x}_j \rangle = n$ if $i=j$

  < 0 if $i \neq j$.

Geometric Lemma : $\exists$ n-dim. vectors $\tilde{x}_1, \dots \tilde{x}_m$ s.t. pairwise angle $> 90^\circ \Rightarrow m < n+1$

(Tightness : Take n+1- dim. simplex)

Proof: (Can prove by induction, but we'll prove by linear algebra.) Say $m \geq n+2$.

Since $\tilde{x}_1 \dots \tilde{x}_{n+1}$ are linearly dependent,

$\exists\ \lambda_1 \dots \lambda_{n+1}$ s.t.

$$\sum \lambda_i \tilde{x}_i = 0$$

Say $\lambda_1 \dots \lambda_\ell > 0$, $\lambda_{\ell+1} \dots \lambda_t < 0$

(& rest are zero)

Case 1: $t > \ell > 0$

Let $$z = \sum_{i=1}^{\ell} \lambda_i \tilde{x}_i = - \sum_{j=\ell+1}^{t} \lambda_j \tilde{x}_j$$

Then

$$0 \leq \langle z, z \rangle = \left\langle \sum \lambda_i \tilde{x}_i , - \sum \lambda_j \tilde{x}_j \right\rangle$$

$$= - \sum_{i,j} \lambda_i \lambda_j \langle \tilde{x}_i , \tilde{x}_j \rangle < 0 \otimes$$

Case 2: $t = \ell > 0$

Then

$$0 = \langle \tilde{x}_{n+2}, 0 \rangle$$

$$= \left\langle \tilde{x}_{n+2}, \sum_{i=1}^{\ell} \lambda_i \tilde{x}_i \right\rangle$$

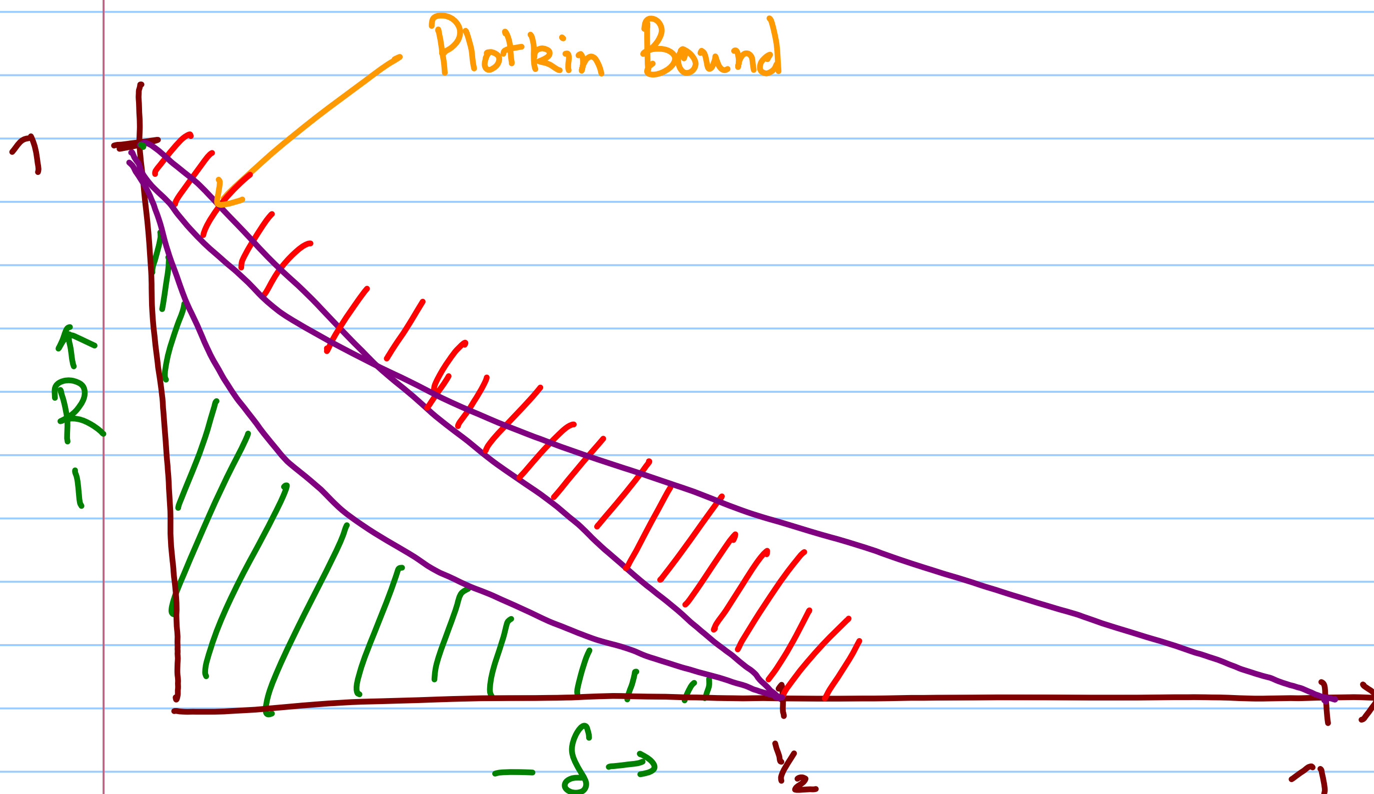
$$= \sum_{i=1}^{\ell} \lambda_i \langle \tilde{x}_i, \tilde{x}_{n+2} \rangle$$

$$< 0 \qquad \otimes$$

In either case get a contradiction, & so $m \leq n+1$.

$\boxtimes$

Updated Graph $(q=2)$

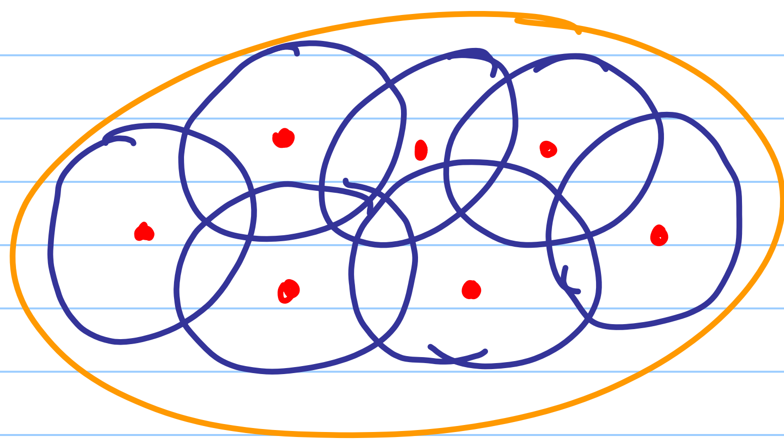


Final Bound(s) : [Elias - Bassalygo] bound

Motivation : Single bound that is better than Hamming + Plotkin.

Idea:

- Improve on Hamming bound by drawing <u>larger</u> balls around each codeword



- Balls no longer disjoint but may have small "overlap."
- Say T such that no point contained in more than $L = \text{poly}(n)$ balls.
- Then $$2^k \cdot 2^{H(T)n} \leq L \cdot 2^n$$

$$\Rightarrow \quad R + H(T) \leq 1$$

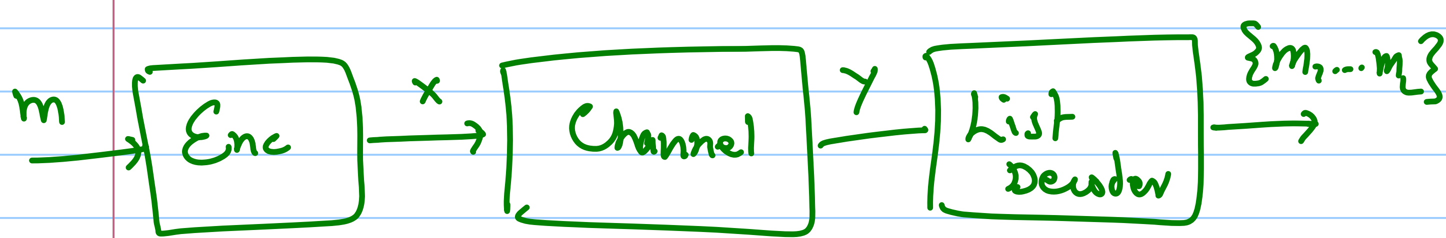
larger ↑ ↑ No change

How large can balls be so that they have little overlap?

Radius = "List-decoding radius"

LIST-DECODABILITY OF CODES

- Alternate notion of recovery from errors



Success? = "$m \in \{m_1, \dots, m_L\}$"?

- Decoder outputs (small) list of messages.
- Transmission "successful" if sender's message included in decoder's list.
- Is list-decodability better than "unique-decodability"?

Johnson's Bound

Thm: Code of distance δ has list-decoding radius

$$\tau = \frac{1}{2}\left(1 - \sqrt{1-2\delta}\right)$$

$\Big\}$ $(q=2)$

Proof: Geometric. Exercise. Omitted.

Consequequence:

Elias-Bassalygo Bound

$$R + H\left(\frac{1}{2}\left(1-\sqrt{1-2\delta}\right)\right) \leq 1$$

- Clearly better than Hamming
- Also better than Plotkin

$$\frac{1}{2}\left(1-\sqrt{1-2\delta}\right) ?$$

- $(1-x)^{1/2} \leq 1-\frac{x}{2}$

$$\Rightarrow \frac{1}{2}\left(1-\sqrt{1-2\delta}\right) \geq \frac{\delta}{2} \quad \text{-------- } 1$$

- $\delta \to 0 \Rightarrow \frac{1}{2}\left(1-\sqrt{1-2\delta}\right) \longrightarrow \frac{\delta}{2}$ ---- 2

- $\delta \to \frac{1}{2}$? say $\delta = \frac{1}{2} - \epsilon$, $\epsilon \to 0$

$$\frac{1}{2}\left(1-\sqrt{1-2\delta}\right) = \frac{1}{2}\left(1-\sqrt{2\epsilon}\right)$$

$$H\left(\frac{1}{2}-\alpha\right) \approx \Theta(\alpha^2) \quad \left[\text{when } \alpha = o(1)\right]$$

& so: $H\left(\frac{1}{2}\left(1-\sqrt{1-2\delta}\right)\right) = H\left(\frac{1}{2}\left(1-\sqrt{2\epsilon}\right)\right)$

$$= \Theta(\epsilon)$$

$R \leq 1 - \Theta(\epsilon)$ Is this tight?

SURVEY

- Best codes we know so far ($q=2$) are random codes / Greedy codes
- Achieve $R = 1 - H(\delta)$
- when $\delta \to 0$

$$R = 1 - \delta \log_2 \frac{1}{\delta}$$

upper bound [Hamming / Elias] which is correct?

$$R \leq 1 - \frac{1}{2} \cdot \delta \log \frac{1}{\delta}$$

- when $\delta = \frac{1}{2} - \epsilon$ & $\epsilon \to 0$

$$R \geq \frac{1}{2} - O(\epsilon^2)$$

upper bound Elias / Plotkin : $R \leq \frac{1}{2} - \Omega(\epsilon)$

better upper bound "LP Bound" : $R \leq \frac{1}{2} - \tilde{O}(\epsilon^2)$

... Alas, LP Bound out of scope for us.

APPENDIX: JOHNSON BOUND

Question: if C has distance δ, then what is a radius τ s.t. every ball of radius τ has few codewords?

[should hold $\forall$ code C w. $\delta(C) \geq \delta$]

Thoughts:

① Certainly τ can be $\frac{\delta}{2}$, but can it be larger?

② Can $\tau > \delta$? Converse Shannon $\Rightarrow$ NO!

③ Can $\tau \to \delta$?

Not really... as we argue below

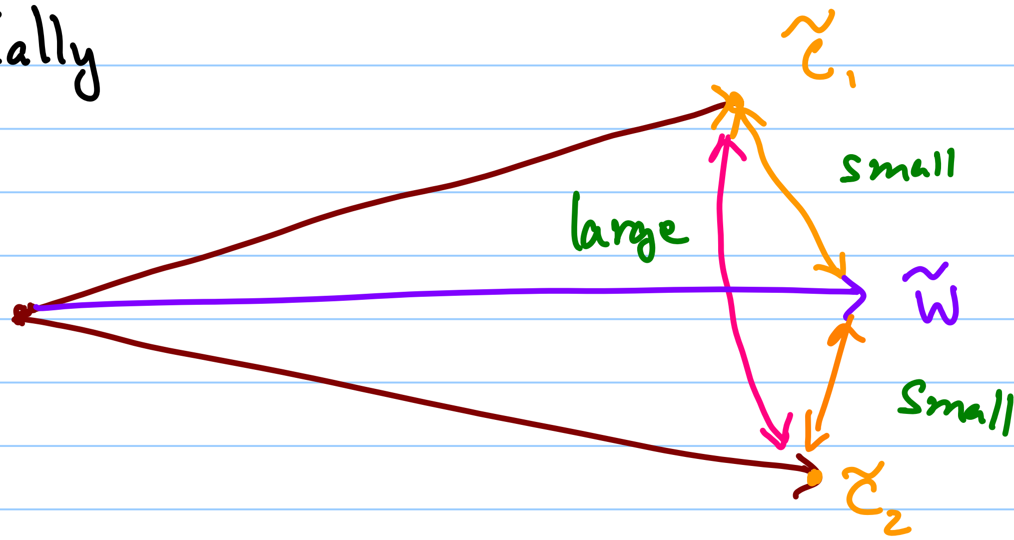
- Pick random words from
  Ball$(\bar{0}, \tau \cdot n)$
- Expected distance $\approx \underbrace{2\tau(1-\tau)n}_{\text{why?}}$
- Setting $2\tau(1-\tau) = \delta$ we get
  $$\tau = \frac{1}{2}\left(1 - \sqrt{1-2\delta}\right) \ldots$$
- So $\exists C$ of distance δn s.t.
  all codewords in Ball$(\bar{0}, \tau n)$,
  & C has $\exp(n)$ codewords
- Is this right? Johnson bound $\Rightarrow$ YES!

Proof of Johnson Bound :

- Say $c_1 \ldots c_m$ codewords of C
  - $\Delta(c_i, c_j) \geq \delta n$
  - $\Delta(c_i, w) \leq \tau n$

- Hamming $\longrightarrow$ Euclid : $\tilde{c}_1, \ldots \tilde{c}_m, \tilde{w}$ s.t.
  - $\langle \tilde{c}_i, \tilde{c}_i \rangle = \langle \tilde{w}, \tilde{w} \rangle = n$
  - $\langle \tilde{c}_i, \tilde{c}_j \rangle \leq (1-2\delta) \cdot n$
  - $\langle \tilde{c}_i, \tilde{w} \rangle \geq (1-2\tau) \cdot n$

- Pictorially



- How many such brown vectors can exist in small dimension?

- Can reduce to previous question by shifting origin to $\alpha \cdot \tilde{w}$, where $0 \le \alpha \le 1$.

- Can we find such α, so that

$$\langle \tilde{c}_i - \alpha \tilde{w}, \tilde{c}_j - \alpha \tilde{w} \rangle < 0 \ ?$$

- Straightforward algebra ....
  can do it if

$$2\tau(1-\tau) < \delta \; .$$

- Thence .... Johnson Bound.