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 $\mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$ with $\Delta(C) \geq d$, $|C| = q^k$

- $[\cdot \; \cdot \; \cdot ] \Rightarrow$ linear code

- $q=2 \Rightarrow$ code with $k \geq n - \log_2 \text{Vol}(n, d)$

- $R \triangleq \frac{k}{n}$; $S = \frac{d}{n}$;

  $\Rightarrow$ code with $R \geq 1 - H(S)$
A simple bound [Singleton]:

**Theorem:** \( \forall q \; R + S \leq 1 \)

\[ \iff k + d \leq n + 1 \]

**Proof:** Project all codewords to first \( k-1 \) word.

Projection function \( \Pi : \leq \rightarrow \leq \)

Sine \# codewords \( \geq \binom{n}{k-1} \)

\( \exists \) distinct codewords \( x, y \) s.t.

\[ \Pi(x) = \Pi(y) \]

\[
\begin{array}{|c|c|c|}
\hline
\alpha & p & x \\
\hline
k-1 & \rightarrow \\
\hline
\alpha & p' & y \\
\hline
\end{array}
\]

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

\[ \Rightarrow c_1 \leq n - k + 1. \]

Can we do better? For \( q=2 \)?
Recall

- Code of distance $8$ corrects $\frac{8}{2}$ errors
  $$\Rightarrow \exists \text{ codes correcting } \frac{8}{2} \text{ fraction of errors}$$
  with rate $R \geq 1 - H(\frac{8}{2})$

- Contrast with [Shannon] who guaranteed codes correcting $\frac{8}{2}$ fraction random, independent, errors with rate $R \geq 1 - H(\frac{8}{2})$. [higher rate!]

- [Shannon] Converse: $R \leq 1 - H(\frac{8}{2})$.

[Hamming’s]: Also proved $R \leq 1 - H(\frac{8}{2})$. 
**Hamming Bound**

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

**Conclusion:**

$$2^R \cdot \text{Vol}(n, \frac{d-1}{2}) \leq 2^n$$

$$\Rightarrow R + \log_2 \text{Vol}(n, \frac{d-1}{2}) \leq n$$

$$\Rightarrow R + H\left(\frac{\xi}{2}\right) \leq 1 \quad [q=2]$$
Is the x-intercept right?

Can we really have codes with $s = 0.75$?

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

\[ R + 2s \leq 1 \]

(i) \[ d > \frac{n}{2} \implies k \leq \log_2 n + 1 \]

(ii) \[ \exists (n, k, d) \text{ code} \implies \exists (n-1, k-1, d) \text{ code} \]

\[ \exists (n-1, k, d-1) \text{ code} \]

Proof of (ii):

- Say $C$ is an $(n, k, d)$ code

- Let $C_0$ be all codewords ending with 0

\[ C, \ldots, C_k \]
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 $\geq d$

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

Let $\tilde{C}$ be projection of $C$

to last $n-1$ coords.

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

message length $\geq k$

distance $\geq d-1$

$\blacklozenge (ii)$
Proof of (i): Hamming $\rightarrow$ Euclid

**Idea:**
- Map $\Sigma$ to Euclidean space...
- Hamming distance maps to $\ell_2$ distance
- Extend map to $\Sigma^n$ & derive coding theory bounds from these.

**Step 1:** $\mathbb{E}_0,1^1 \rightarrow \mathbb{R}^1$

0 $\rightarrow$ 1

1 $\rightarrow$ -1

**Step 2:** $\mathbb{E}_0,1^n \rightarrow \mathbb{R}^n$

$x \rightarrow \tilde{x}$

$\Delta(x,y) = d \Rightarrow \langle \tilde{x}, \tilde{y} \rangle = n - 2d$
"Now the coding theory:

- Suppose $C = \{x_1, \ldots, x_m\} \subseteq \{0,1\}^n$
  
  with $\Delta(x_i, x_j) > \frac{n}{2}$

- Euclidean version $\mathcal{C} = \{\tilde{x}_1, \ldots, \tilde{x}_m\} \subseteq \mathbb{R}^n$
  
  with $\langle \tilde{x}_i, \tilde{x}_j \rangle = n$ if $i=j$
  
  $< 0$ if $i \neq j$.

**Geometric Lemma**: There exist $n$-dim. vectors $\tilde{x}_1, \ldots, \tilde{x}_m$ such that for any $i \neq j$:

- pairwise angle $\geq 90^\circ$ implies $m < n+1$

(Tightness: Take $n+1$-dim. simplex)
Proof: (can prove by induction, but we'll prove by linear algebra.) Say \( m \geq n+2 \).

Since \( \tilde{x}_1, \ldots, \tilde{x}_{n+1} \) are linearly dependent,

\[ \exists \lambda_1, \ldots, \lambda_{n+1} \text{ s.t.} \]

\[ \sum \lambda_i \tilde{x}_i = 0 \]

by \( \lambda_1, \ldots, \lambda_{n+1} \geq 0 \), \( \lambda_{n+1}, \ldots, \lambda_{n+1} < 0 \)

\( (\text{all rest are zero}) \)

Case 1: \( t > l > 0 \)

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

Then

\[ 0 \leq \langle z, z \rangle = \sum \lambda_i \lambda_j \langle \tilde{x}_i, \tilde{x}_j \rangle \]

\[ = - \sum \lambda_i \lambda_j \langle \tilde{x}_i, \tilde{x}_j \rangle < 0 \]
Case 2: $t = l > 0$

Then

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

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

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

$$< 0 \quad \big\times$$

In either case get a contradiction, $\therefore m \leq n+1$.  \[\square\]
Updated Graph \((q=2)\)

Plotkin Bound

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

Motivation: Single bound that is better than Hamming + Plotkin.
Idea:
• Improve on Hamming bound by drawing larger 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 $2^k \cdot 2^{H(T)n} \leq L \cdot 2^n$

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

$\uparrow$ No change

$\downarrow$ larger
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

\[ m \xrightarrow{\text{Enc}} \xrightarrow{x} \xrightarrow{\text{Channel}} \xrightarrow{\text{List Decoder}} \{m_1, \ldots, m_\ell\} \]

Success? = "\( m \in \{m_1, \ldots, m_\ell\} \)?

- 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 $d$ has list-decoding radius \( r \)\( (q=2) \)

\[
T = \frac{1}{2} (1 - \sqrt{1-2r})
\]

**Proof:** Geometric. Exercise. Omitted.

**Consequence:**

**Elias-Bassalygo Bound**

\[
R + H\left(\frac{1}{2} (1 - \sqrt{1-2r})\right) \leq 1
\]

- Clearly better than Hamming
- Also better than Plotkin
\[ \frac{1}{2} \left( 1 - \sqrt{1 - 2\delta} \right) \]

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

\[ \Rightarrow \frac{1}{2} \left( 1 - \sqrt{1 - 2\delta} \right) \geq \frac{\delta}{2} \] \hspace{1cm} \text{(1)}

\[ \delta \to 0 \Rightarrow \frac{1}{2} \left( 1 - \sqrt{1 - 2\delta} \right) \to \frac{\delta}{2} \] \hspace{1cm} \text{(2)}

\[ \delta \to \frac{1}{2} \text{?} \text{ say } \delta = \frac{1}{2} - \varepsilon, \varepsilon \to 0 \]

\[ \frac{1}{2} \left( 1 - \sqrt{1 - 2\delta} \right) = \frac{1}{2} \left( 1 - \sqrt{2\varepsilon} \right) \]

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

\[ \Rightarrow \quad H\left( \frac{1}{2} \left( 1 - \sqrt{1 - 2\delta} \right) \right) = H\left( \frac{1}{2} \left( 1 - \sqrt{2\varepsilon} \right) \right) \]

\[ = \Theta(\varepsilon) \]

\[ R \leq 1 - \Theta(\varepsilon) \text{ Is this tight?} \]
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 / Eliáš] which is correct?

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

- When $\delta = \frac{1}{2} \cdot \epsilon \quad \epsilon \to 0$

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

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

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

... Also, LP Bound out of scope for us.
Appendix: Johnson Bound

Question: if C has distance $s$, then what is a radius $T$ s.t. every ball of radius $T$ has few codewords? [should hold a code C w. $8(c) \geq s$]

Thoughts:

1. Certainly $T$ can be $\frac{s}{2}$, but can it be larger?

2. Can $T \rightarrow s$? Converse Shannon $\Rightarrow$ NO!

3. Can $T \rightarrow \infty$? Not really... as we argue below
- Pick random words from $\text{Ball}(\hat{0}, \tau \cdot n)$

- Expected distance $\approx 2\tau(1-\tau)n$

  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 $\delta n$ s.t.

  all codewords in $\text{Ball}(\hat{0}, \tau \cdot n)$,

  & $C$ has $\exp(n)$ codewords

- Is this right? Johnson bound $\Rightarrow$ YES!
Proof of Johnson Bound:

- Say $c_i, \ldots, c_m$ codewords of $C$
  - $\Delta(c_i, c_j) \geq 8n$
  - $\Delta(c_i, w) \leq Tn$

- Hamming $\rightarrow$ Euclid: $\tilde{c}_1, \ldots, \tilde{c}_m, \tilde{w}$ s.t.
  - $\langle \tilde{c}_i, \tilde{c}_i \rangle = \langle \tilde{w}, \tilde{w} \rangle = \eta$
  - $\langle \tilde{c}_i, \tilde{c}_j \rangle \leq (1 - 28) \cdot \eta$
  - $\langle \tilde{c}_i, \tilde{w} \rangle \geq (1 - 2T) \cdot \eta$
Pictorially

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

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

- Can we find such $\alpha$, so that
  
  $\langle \tilde{z}_i - \alpha \tilde{w}, \tilde{z}_j - \alpha \tilde{w} \rangle < 0$
- Straightforward algebra....
  can do it if
  \[ 2^r (1-r) < s. \]

- Hence ... Johnson Bound.