Today
- Coding Bounds
  - ★ Singleton
  - ★ Plotkin
  - ★ Elias-Bassalygo

CS3.318.1
Coding Theory
Lecture 5 (2022-9-14)
Instructor: Prahladh
Harsha.

Let's recap:

What we can do

GV bound: If n, d are any positive integers then $\exists$ $(n,k,d)_2$-code C st

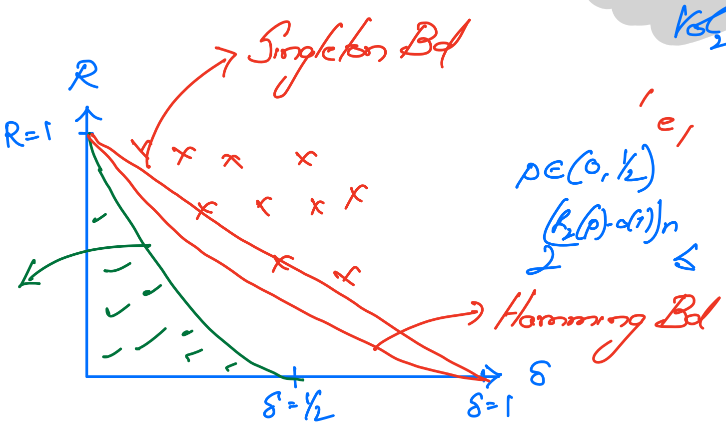
$$2^k \geq \frac{2^n}{|Vol_2(n,d-1)|}$$

ie, $R \geq 1 - h_2(\delta)$

What we cannot do:

Hamming bound: If C is a $(n,k,d)_2$-code then

$$2^k \leq \frac{2^n}{Vol_2(n, \lfloor\frac{d-1}{2}\rfloor)}$$



ie, $R \leq 1 - h_2(\delta/2) + o(1)$

$\rho \in (0, 1/2)$

$$2^{(h_2(\rho) - o(1))n} \leq Vol(n, \rho n) \leq 2^{h_2(\rho) n}$$

Singleton Bound: $\forall$ $(n,k,d)_q$-code, we have

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

Pf: $\mathcal{C}$ is $(n,k,d)_q$-code $\quad \mathcal{C} \subseteq \Sigma^n$, $|\Sigma| = q$

$|\mathcal{C}| = q^k$

Projection: $\Sigma^n \xrightarrow{\pi} \Sigma^{k-1}$ (formed by dropping all of the first $n-k+1$ symbols).

By PHP, $\exists$ $c_1 \neq c_2 \in \mathcal{C}$, s.t $\pi(c_1) = \pi(c_2)$

$$\Delta(c_1, c_2) \leq n-k+1$$

Hence, $d \leq n-k+1$ ⊠

In the asymptotic notation. $R + \delta \leq 1 + o(1)$.

—

For every fixed alphabet q, Singleton bd is worse than Hamming bd.

But surprisingly, will construct codes which meet Singleton bd (albeit over a growing alphabet)

—

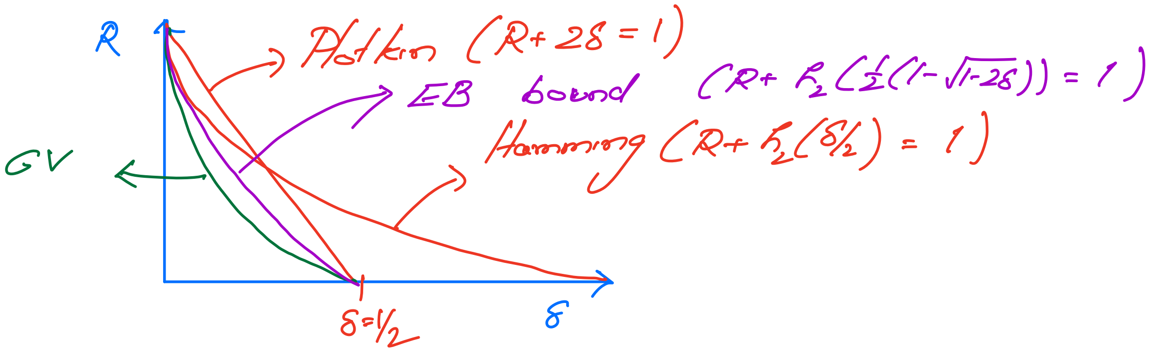
Plotkin Bound: $\mathcal{C}$ is $(n,k,d)_2$-code.

1. $d > \frac{n}{2} \Rightarrow |\mathcal{C}| \le n+1$

2. For any d, $|\mathcal{C}| \le 2d \cdot 2^{n-2d+1}$.

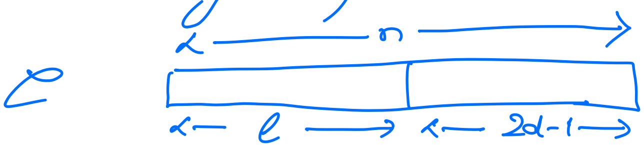
In the asymptotic notation $2^k \le 2^{n-2d+2+\log_2 d}$

ie, $R \le 1-2\delta+o(1)$



Proof of Plotkin Bd.

(2) (assuming (1))



where $\ell = n-2d+1$

For every $a \in \{0,1\}^\ell$, $\mathcal{C}_a = \{x \in \mathcal{C} \mid x = ay$ for some $y \in \{0,1\}^{2d-1}\}$

Obs: $\Delta(\mathcal{C}_a) \ge d$, $\forall a$

Hence by (1), $|\mathcal{C}_a| \le 2d-1+1 = 2d$.

$|\mathcal{C}| = \sum_a |\mathcal{C}_a| \le 2^\ell \cdot 2d$ (end of part (2))

(1) Proof of part (1).

(i.e, $d > n/2 \Rightarrow |\mathcal{C}| \leq n+1$).

Geometric Technique: Hamming $\longrightarrow$ Euclid.

$$\{0,1\} \longrightarrow \mathbb{R}$$

$$b \longmapsto (-1)^b = \tilde{b}$$

i.e, $\begin{cases} 0 \longmapsto 1 \\ 1 \longmapsto -1 \end{cases}$

Extend $\{0,1\}^n \longrightarrow \mathbb{R}^n$

$$(x_1, \ldots x_n) \longmapsto (\tilde{x}_1, \tilde{x}_2, \ldots \tilde{x}_n)$$

Fact: $\Delta(x,y) = d$, iff $\langle \tilde{x}, \tilde{y} \rangle = n - 2d$.

$$\hookrightarrow \sum \tilde{x}_i \tilde{y}_i$$

$\mathcal{C} = \{c_1, \ldots c_m\} \subseteq \{0,1\}^n \longmapsto \tilde{\mathcal{C}} = \{\tilde{c}_1, \ldots \tilde{c}_m\} \subseteq \mathbb{R}^n$

$\Delta(\mathcal{C}) > n/2$

$\forall i \neq j \quad \langle \tilde{c}_i, \tilde{c}_j \rangle < 0$

$\forall i, \quad \langle \tilde{c}_i, \tilde{c}_i \rangle = n$

$|\tilde{\mathcal{C}}| \leq n+1$

(tight: vertices of a simplex in n-dim).

Geometric Lemma: If $z_1, \ldots z_m \in \mathbb{R}^n$ s.t $\forall i \neq j \quad \langle z_i, z_j \rangle < 0$, then $m \leq n+1$

Pf: Assume otherwise

ie, $\exists\ z_1, z_2, \ldots\ z_{n+2} \in \mathbb{R}^n$, st $\langle z_i, z_j\rangle < 0\ \forall i \neq j$

$z_1, \ldots\ z_{n+1} \in \mathbb{R}^n$ and hence linearly dependent

ie, $\sum_{i=1}^{n+1} \lambda_i z_i = 0$ for some $(\lambda_1, \ldots\ \lambda_{n+1}) \neq 0^{n+1}$

wlog. assume $\exists\ 0 < l \leq t \leq n+1$

$$z := \sum_{i=1}^{l} \alpha_i z_i = \sum_{j=l+1}^{t} \beta_j z_j \qquad \alpha_i, \beta_j > 0$$

Case(i) $l < t$

$$0 \leq \langle z, z\rangle = \sum_{i=1}^{l} \sum_{j=l+1}^{t} \alpha_i \beta_j \langle z_i, z_j\rangle < 0 \quad \Rightarrow\Leftarrow$$

Case(ii) $l = t$ $\qquad z = 0$

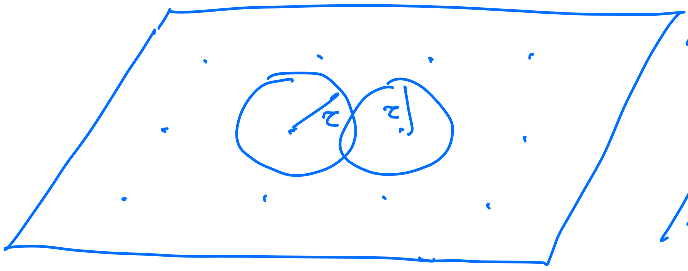
$$0 = \langle z_{n+2}, z\rangle = \sum_{i=1}^{l} \alpha_i \langle z_{n+2}, z_i\rangle < 0 \quad \Rightarrow\Leftarrow$$

☒

Qn: Is there a "nice" bd that performs as well as Plotkin & Hamming.

Ans: Yes, Elias-Bassalygo bound.

Elias-Bassalygo Bound.



$\{0,1\}^n$. Suppose $\exists\ \tau, L$ s.t. $\forall x \in \{0,1\}^n$ $|Ball(x, \tau n) \cap \mathcal{C}| \le L$.

$$|\mathcal{C}| \cdot Vol_2(n, \tau n) \le L \cdot 2^n$$

$$k + h_2(\tau) n \le 1 + \log_2 L$$

$$R + h_2(\tau) \le 1 + \frac{\log L}{n}$$

Obs: As long as $L = 2^{o(n)}$, we get $R + h_2(\tau) \le 1 + o(1)$.

→ List-decoding (as opposed to unique decoding).

— Johnson Radius: $\delta \in (0, 1/2)$

$\forall$ codes $\mathcal{C}$ $(n, k, \delta n)_2$-code,

$$J_2(\delta) = \frac{1}{2}\left(1 - \sqrt{1-2\delta}\right)$$

$\forall c \in \mathcal{C}$, $|Ball(c, J_2(\delta) n) \cap \mathcal{C}| = poly(n)$.

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

$\sqrt{1-2\delta} \le 1-\delta$

$\frac{1}{2}(1-\sqrt{1-2\delta}) \ge \delta/2$

Cor: EB bound

$$R + h_2(J_2(\delta)) \le 1 + o(1).$$

(By design, EB is better than Hamming

By convexity arguments, EB is better than Plotkin.

$\delta \to 0.$

$J_2(\delta) \to \delta/2$

$R \le 1 - h_2(\delta/2)$

$= 1 - \frac{\delta}{2} \log \frac{1}{\delta}$ (EB)

$\delta = 1/2 - \varepsilon \qquad \varepsilon \to 0$

$(\frac{1}{2}(1-\sqrt{1-2\delta})) = (\frac{1}{2}(1-\sqrt{2\varepsilon}))$

$h_2(\frac{1}{2}-\alpha) = 1 - \Theta(\alpha^2)$ for small $\alpha = o(1)$

$R = O(\varepsilon)$ (EB bd)

Achievability:

GV: $R \ge 1 - h_2(\delta)$

which is correct

$\exists C,\quad R \ge 1 - \delta \log \frac{1}{\delta}$

GV: $R \ge 1 - h_2(\delta)$

$\exists C,\ R = \Omega(\varepsilon^2)$

LP-bound (MRRW)

$R = O(\varepsilon^2 \log \frac{1}{\varepsilon})$