E2 205 Error-Control Coding
Lecture 9

Srinivas Vankudothu

September 11, 2019

1 Hamming Bound

$$M_n \leq \frac{2^n}{\sum_{i=0}^{t_{\mathrm{n}}} \binom{n}{i}}$$

$$\text{where} \quad t_{\mathrm{n}} = \left\lfloor \frac{d_n - 1}{2} \right\rfloor \quad and \;\; \mathrm{d_n} = d_{\min} \text{ at length n.}$$

2 Asymptotic Hamming Bound

$$R \leq 1 - H_2(\delta/2)$$

Essentially since,

$$\lim_{n\to\infty} \frac{\log_2 \sum_{i=0}^{t_{\mathrm{n}}} \binom{n}{i}}{n} = H_2\left(\lim_{n\to\infty} \frac{t_{\mathrm{n}}}{n} \right)$$

$$\mathrm{A}s \;\; d_n = (n\delta) \;\; so \;\; \lim_{n\to\infty} \frac{d_n}{n} = \delta$$

3 Gilbert-Varshamov Bound

$$M_{\mathrm{n}} \leq \frac{2^n}{\sum_{i=0}^{d_{\mathrm{n}}-1} \binom{n}{i}}, \;\; where \;\; d_{\mathrm{n}} = d_{\min}.$$

4 Asymptotic G-V Bound

$$R \geq 1 - H_2(\delta)$$

(Via a similar bound)

Over the BSC can achieve

$$R \geq 1 - H_2(2\epsilon)$$

. But the channel capacity is given by

$$C = 1 - H_2(\epsilon)$$

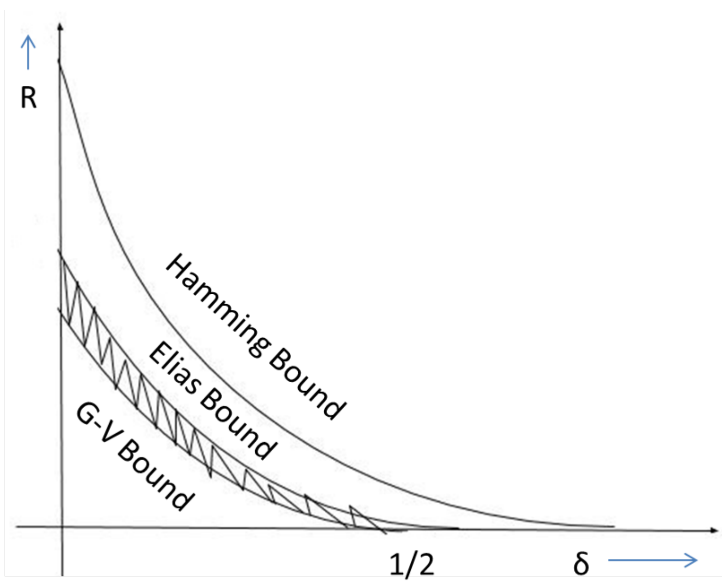

Figure 1: Bounds

5 Plotkin Bound

Main goal is to show that R(δ)=0, when $\delta \geq 1/2$.

Proof. Let $\mathcal{C}$ an (n, M, d) code with $d = d_{\mathrm{min}} \geq \frac{n}{2}$ i.e, $2d > n$.
Consider the matrix A_{Mxn}, whose M rows are code words of $\mathcal{C}$. Let the Hamming weight of the i^{th} column be w_{i}.

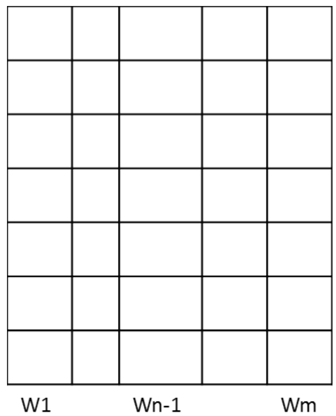

Figure 2: Matrix A

Therefore total Hamming weight of A is $\sum_{i=1}^{n} w_{\mathrm{i}}$.

Let $\triangle_{\mathrm{ij}}$ be the Hamming distance between the i^{th} and j^{th} rows of A. Then,

$$\sum_{1 \leq i < j \leq n} \triangle_{\mathrm{ij}} = \sum_{i=1}^{n} w_{\mathrm{i}}(M - w_{\mathrm{i}})$$

Example:

1	0	1	1
0	1	1	1
0	1	1	0

Figure 3: Example matrix

$$\sum_{1 \leq i < j \leq n} \triangle_{\mathrm{ij}} = 2 + 3 + 1 = 6$$

$$\sum_{i=1}^{n} w_{\mathrm{i}}(M - w_{\mathrm{i}}) = 2 + 2 + 0 = 6$$

Note that,

$$\max_{0 \le w \le M} w(M - w) = \begin{cases} \frac{M^2}{4}, & \text{if M is odd,} \\ \left(\frac{M-1}{2}\right)\left(\frac{M+1}{2}\right), & \text{if M is even.} \end{cases}$$

Also,

$$\sum_{j \ge i} \triangle_{\mathrm{ij}} \ge \binom{M}{2} d$$

- M is even case

$$\begin{aligned} \binom{M}{2} d \le \sum_{j>i} \triangle_{\mathrm{ij}} &\le \frac{nM^2}{4} \\ \frac{M(M-1)}{2} d &\le \frac{nM^2}{4} \\ 2(M-1)d &\le nM \\ M(2d - n) &\le 2d \\ M &\le \frac{2d}{2d - n} \end{aligned}$$

- M is odd case

$$\begin{aligned} \binom{M}{2} d &\le \frac{n(M^2 - 1)}{4} \\ \left(\frac{M(M-1)}{2}\right) d &\le \frac{n(M^2 - 1)}{4} \\ 2Md &\le n(M + 1) \\ M(2d - 1) &\le n \\ M \le \frac{n}{2d - n} &\le \frac{2d}{2d - n} \end{aligned}$$

In either case: M $\leq \frac{2d}{2d-n} = \frac{2\delta}{2\delta-1}$ where $\delta = \frac{d}{n}$.

$$\limsup_{n\to 0} \log_2(M_{\mathrm{n}}) = \lim_{n\to\infty} \frac{\log(\frac{2\delta}{2\delta-1})}{n} = 0$$

$\square$

6 Elias Bound

- Let $\mathcal{C}$ be an (n, M, d) code with $d \leq \frac{n}{2}$.
- Let $t \leq \frac{n}{2}$ be an integer.

$$\sum_{\underline{x}\in\mathbb{F}_2^n} |\mathcal{B}(\underline{x}, t) \cap \mathcal{C}| = \sum_{\underline{c}\in\mathcal{C}} |\mathcal{B}(\underline{c}, t)|$$

- For some $\underline{x} \in \mathbb{F}_2^n$ we must have

$$|\mathcal{B}(\underline{x}, t) \cap \mathcal{C}| \geq \frac{|\mathcal{B}(\underline{0}, t)||\mathcal{C}|}{2^n} = \frac{\sum_{i=0}^{t} \binom{n}{i} M}{2^n}$$

- From this we know that the existence of an (n, M, d) code implies the existence of a code $\mathcal{C}_0$ that contains $\geq \frac{\sum_{i=0}^{t}\binom{n}{i}M}{2^n}$ code words in a ball of radius t surrounding the origin.

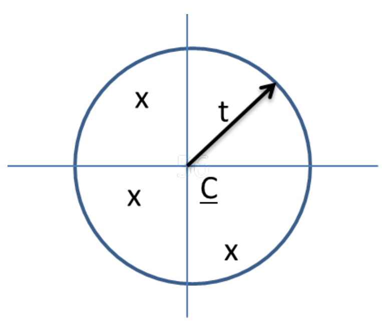

Figure 4: Ball of radius t

- On the other hand, let p be the maximum number of binary n-tuples contained in a ball of radius t surrounding the origin such that any 2 are Hamming distance atleast d apart. Form a $(p \times n)$ matrix as before and we have

$$\sum_{j>i} \triangle_{\mathrm{ij}} \geq \binom{p}{2} d$$

  Also

$$\sum_{j>i} \triangle_{\mathrm{ij}} = \sum_{j=i}^{n} w_{\mathrm{i}}(p - w_{\mathrm{i}})$$

Let

$$\sum_{j=i}^{n} w_{\mathrm{i}} = pf, \quad \text{where f is average weight of the row } (f \leq t).$$

Note from the Cauchy Schwarz inequality that

$$|\sum_{i=1}^{n} w_{\mathrm{i}}| = |\underline{w}^{\mathrm{T}} \underline{1}| \leq ||w|| \, ||\underline{1}||$$

$$|\sum_{i=1}^{n} w_{\mathrm{i}}| \leq \sqrt{\left(\sum_{i=1}^{n} {w_{\mathrm{i}}}^2\right)} \sqrt{\left(\sum_{i=1}^{n} 1^2\right)}$$

$$\frac{(pf)^2}{n} \leq \sum_{i=1}^{n} {w_{\mathrm{i}}}^2$$

$$p^2 f - \sum_{i=1}^{n} {w_{\mathrm{i}}}^2 \leq p^2 f - \frac{(pf)^2}{n}$$

$$\sum_{j>i} \triangle_{\mathrm{ij}} = \sum_{j=i}^{n} w_{\mathrm{i}}(p - w_{\mathrm{i}}) = p^2 f - \sum_{i=1}^{n} {w_{\mathrm{i}}}^2$$

$$\therefore \binom{p}{2} d \leq p^2 f - \frac{(pf)^2}{n}$$

$$\left(\frac{p(p-1)}{2}\right)d \le p^2 f - \frac{(pf)^2}{n}$$

$$(p-1)d \le 2pf(1-\frac{f}{n})$$

$$p(d-2f+2\frac{f^2}{n}) \le d$$

$$p \le \frac{nd}{nd-2nf+2f^2}$$

$$p \le \frac{2nd}{(n-2t)^2 - n(n-2d)}$$

$$\text{Let } J(\delta) \triangleq \frac{1}{2}(1-\sqrt{1-2\delta})$$

$$\text{Set } \ t = nJ(\delta) - 1$$

$$\frac{t}{n} \le J(\delta)$$

$$n - 2t \ge n\sqrt{1-2\delta}$$

$$\text{Then } \ (n-2t)^2 - n(n-2d) \ge 0$$

But it is an integer,

$$\therefore \ \ (n-2t)^2 - n(n-2d) \ge 1$$

$$\therefore \ \ p \le 2nd, \ \text{when } t = nJ(\delta) - 1$$

$$\therefore \ \ \frac{M\sum_{i=1}^{t}\binom{n}{i}}{2^n} \le p \le 2nd$$

$$M \le \frac{2^n 2nd}{\sum_{i=1}^{t}\binom{n}{i}}$$

Figure 5: BSC

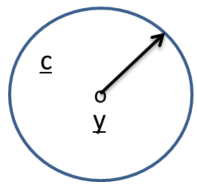

Figure 6: Bounded Distance Decoder

7 Asymptotic Elias Bound

$$\limsup_{n\to\infty} \frac{\log_2 M_{\rm n}}{2} \leq 1 - H_2(J(\delta)) = 1 - H_2(\frac{1}{2}(1-\sqrt{1-2\delta}))$$

Let $\mathcal{C}$ be an (n, M, d) binary code and set $t = \frac{d-1}{2}$. Then a bounded distance decoder (BDD) for $\mathcal{C}$ over the BSC is a decoder that adopts the following algorithm.

- Let $\underline{y} \in \mathbb{F}_2^n$ denote the received vector over the BSC. The decoder searches for a codeword lying in the ball B(y,t) centered at $\underline{\text{y}}$. If the ball contains a codeword $\underline{\mathcal{C}}$ it decodes to $\underline{\mathcal{C}}$, else declares a decoding failure.

The BDD approach does not achieve capacity over the BSC since this would mean employing a code having fractional minimum distance $\delta = \frac{d}{n} = 2\epsilon$. This means to achive the capacity we would need that R(δ)=1-H$_2$($\frac{\delta}{2}$).
(i.e We must have a code that asymptotically achieve the Hamming bound but the Elias upper bound which is strictly tighter than the Hamming bound, tells that this is impossible).