E2 205 Error-Control Coding
Lecture 8

Samrat Kundu

September 9, 2019

1 Bounds on code size

Suppose $\mathcal{C}$ is an $[n, k]$ linear perfect code, then we must have

$$2^k = \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}}$$

where $t = \lfloor \frac{d-1}{2} \rfloor$ and $d =$ minimum distance between any two codewords.

$$\implies \boxed{\sum_{i=0}^{t} \binom{n}{i} = 2^{n-k}}$$

- Suppose a case where $n = 23$ and $k = 12$.

$$2^{11} = \binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048$$

  then it suggests that it is a [23,12,7] **Golay code**.

- Only known perfect codes are as follows:
  i. The binary Hamming codes
  ii. The [23,12,7] **Golay code**
  iii. Non-binary Hamming codes

$$\left[\frac{q^m - 1}{q - 1},\ k = n - m,\ d = 3\right]_q$$

  iv. The $[11, 6, 5]_3$ Ternary code

1.1 The Gilbert-Varshamov lower bound

Theorem. *Let M be the largest size of a binary code of block length n and minimum distance $d_{min} = d$, then*

$$M \geq \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}}.$$

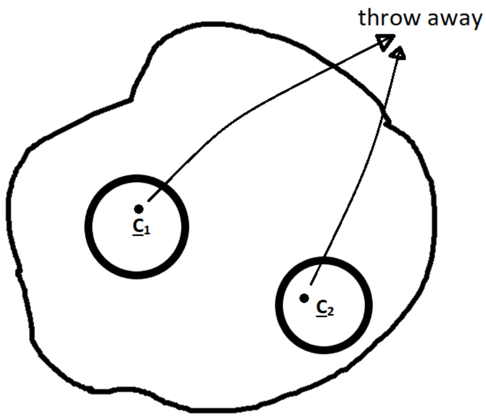

Figure 1: GV Bound

Proof. We follow an iterative procedure from $\mathbb{F}_2^n$. We pick a codeword $\underline{c_i}$ on the i^{th} attempt and throw away all vectors in the ball $\mathcal{B}(\underline{c}_i, d-1)$ and so on. Clearly we will reach a point when there are no more vectors left to pick. Let M be the number of codewords picked up to this point. Then we must have:

$$M|\mathcal{B}(\underline{0}, d-1)| \geq 2^n$$

(else we could pick up one more codeword)

$$\therefore \boxed{M \geq \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}}}$$

□

1.2 Asymptotic $(n \to \infty)$ bounds

Long codes make the channel more predictable and hence causing errors introduced by the channel to be more correctable.

Eg:- Consider the binary symmetric channel. Let the code $\mathcal{C}$ have long blocklength n.

$\mathcal{Q}$: How many errors has the channels introduced?

Set $X_i = 1$, if the i^{th} code symbol is in error
$= 0$, else.

Let,

$$Y_n = \frac{\sum_{i=1}^n X_i}{n}, \qquad \mathbb{E}[Y_n] = \mu.$$

Then,

$$P(|Y_n - \mu| \geq \delta) \leq \frac{\mathbb{E}[(Y_n - \mu)^2]}{\delta^2}.$$

Now,

$$\mathbb{E}[(Y_n - \mu)^2] = \mathbb{E}\Big[\Big(\frac{\sum_{i=1}^n (X_i - \mu)}{n}\Big)^2\Big] = \frac{n\sigma^2}{n^2} = \frac{\sigma^2}{n}, \quad \sigma^2 = \epsilon(1-\epsilon).$$

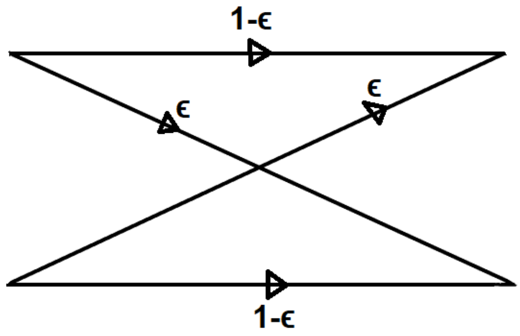

Figure 2: Binary symmetric channel(BSC)

$$\therefore P(|Y_n - \mu| \geq \delta) \leq \frac{\sigma^2}{n\delta^2} \to 0.$$

Set $Z_n = \sum_{i=1}^{n} X_i$, then $Pr(z_n = k) = \binom{n}{k}\epsilon^k(1-\epsilon)^{n-k}$ tends to a Gaussian distribution by the central limit theorem(CLT).

Mean : $\mathbb{E}[Z_n] = n\epsilon$
Standard Deviation : $\sigma = \sqrt{n\epsilon(1-\epsilon)}$

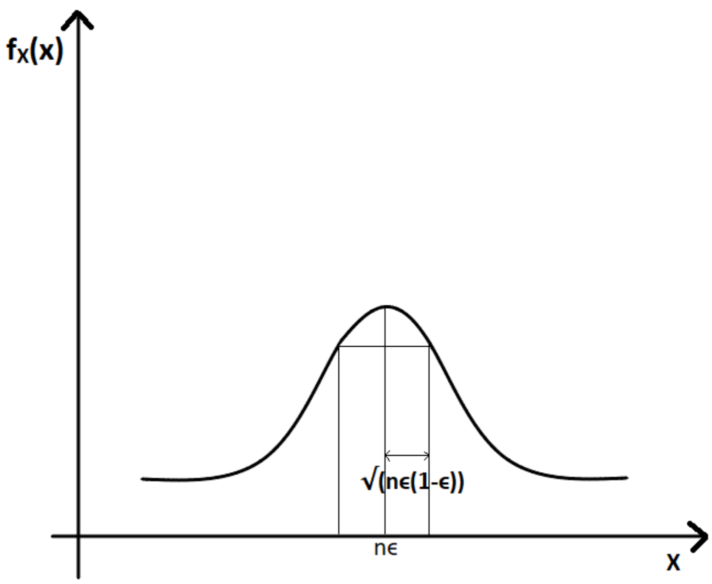

Figure 3: Gaussian distribution with mean and variance as above

Thus with high probability the number of errors is in a narrow band surrounding the mean $n\epsilon$. Thus it suffices to use an error-correcting code with $d_{min} > 2n\epsilon$.
set $\delta = \lim_{n\to\infty}(\frac{d}{n})$ (Fractional minimum distance)
$\implies \delta > 2\epsilon$.

Definition. *Give fractional minimum distance* $0 < \delta < 1$*, let* $d_n = \lceil n\delta \rceil$ *and let* $M(n,\delta)$ *be the largest size of a block code of block length* n *and* $d_{min} = d_n = \lceil n\delta \rceil$*.*

Set rate of the code $= R(\delta) = \limsup_{n\to\infty} \frac{\log_2(M(n,\delta))}{n}$.

$\mathcal{Q}$: How does $R(\delta)$ vary with δ?

Ans: It can be shown that the Hamming and Gilbert-Varshamov bounds imply that

$$1 - H_2(\delta) \leq R(\delta) \leq 1 - H_2\Big(\frac{\delta}{2}\Big)$$

where for $0 < \theta < 1$,

$$H_2(\theta) = \theta \log_2\left(\frac{1}{\theta}\right) + (1-\theta)\log_2\left(\frac{1}{1-\theta}\right) \text{ (The binary entropy function).}$$

Recall,

$$\frac{2^n}{\sum_{i=0}^{d_n-1}\binom{n}{i}} \leq M \leq \frac{2^n}{\sum_{i=0}^{t}\binom{n}{i}}$$

$$\text{For } \ 0 < \mu < \frac{1}{2}, \qquad \frac{2^{nH_2(\mu)}}{\sqrt{8n\mu(1-\mu)}} \leq \sum_{l=0}^{\mu n}\binom{n}{l} \leq 2^{nH_2(\mu)}$$

In our application, $n\mu = d_n - 1$ or $n\mu = t = \lfloor \frac{d_n - 1}{2} \rfloor$.

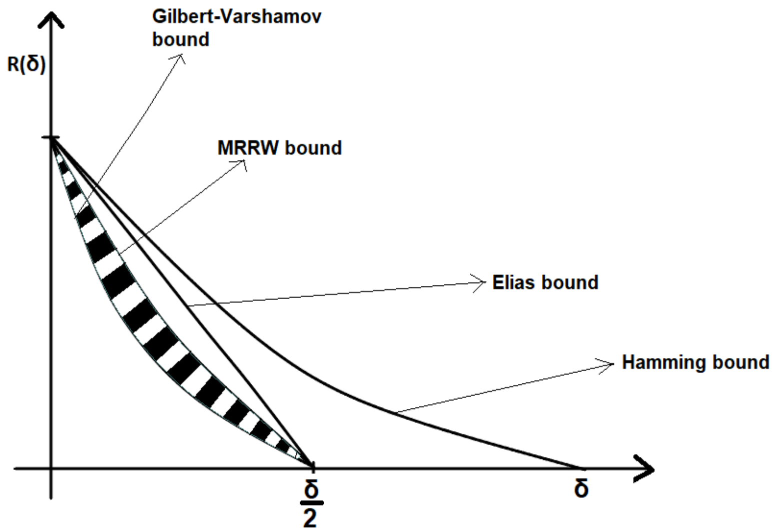

Figure 4: Bounds & relation between rate of the code and fractional minimum distance.(shaded part denotes the region where best code lies)

1.3 The Elias bound

Let $\mathcal{C}$ be a binary code of block length n and minimum distance d.

Let $t \leq \frac{n}{2}$ be an integer.

We want to count the pairs

$$\{\ (\underline{c}, \underline{x}) \mid \underline{c} \in \mathcal{C},\ \underline{x} \in \mathbb{F}_2^n,\ d_H(\underline{c}, \underline{x}) \leq t\ \}$$

in two different ways:

$$\sum_{\underline{x} \in \mathbb{F}_2^n} |\mathcal{B}(\underline{x}, t) \cap \mathcal{C}| = \sum_{\underline{c} \in \mathcal{C}} |\mathcal{B}(\underline{c}, t)| = |\mathcal{B}(\underline{0}, t)||\mathcal{C}|$$

$\therefore$ There must exist $\underline{x} \in \mathbb{F}_2^n$ such that

$$\boxed{|\mathcal{B}(\underline{x}, t) \cap \mathcal{C}| \geq \frac{|\mathcal{B}(\underline{0}, t)||\mathcal{C}|}{2^n}}$$

To be continued...

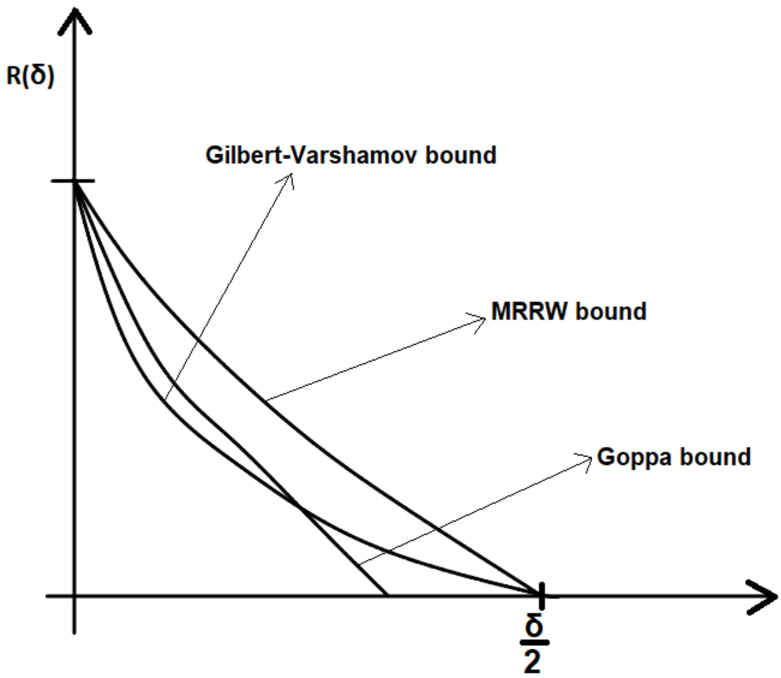

Figure 5: Bounds & relation between rate of the code and minimum fractional distance.