Properties of Linear Block Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

August 7, 2014

Minimum Distance of a Linear Block Code

Definition

The minimum distance of a block code C is defined as

$$d_{min} = \min_{\mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y})$$

Theorem

The minimum distance of a linear block code is equal to the minimum weight of its nonzero codewords

Proof.

$$\begin{aligned} d_{min} &= \min \left\{ \mathrm{wt}(\mathbf{x} + \mathbf{y}) \middle| \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y} \right\} \\ &= \min \left\{ \mathrm{wt}(\mathbf{v}) \middle| \mathbf{v} \in C, \mathbf{v} \neq \mathbf{0} \right\} \end{aligned}$$

Example

Find the minimum distance of a linear block with parity check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Theorem

Let C be a linear block code with parity check matrix $\mathbf{H}$. There exists a codeword of weight w in C $\iff$ there exist w columns in $\mathbf{H}$ which sum to the zero vector.

Corollary

If no $w - 1$ or fewer columns of $\mathbf{H}$ sum to $\mathbf{0}$, the code has minimum distance at least w.

Corollary

The minimum distance of C is the equal to the smallest number of columns of $\mathbf{H}$ which sum to $\mathbf{0}$.

Singleton Bound

Let C be an (n, k) binary block code with minimum distance d_{min}.

$$d_{min} \leq n - k + 1$$

Proof.

Suppose C is a linear block code.

- What is the rank of $\mathbf{H}$?

Suppose C is not a linear block code.

- Puncture the first $d_{min} - 1$ locations in each codeword.
- Can two punctured codewords be the same?

Error Detection using Linear Block Codes

- Suppose an (n, k, d_{min}) linear block code C is used for error detection
- Let $\mathbf{x}$ be the transmitted codeword and $\mathbf{y}$ is the received vector

$$\mathbf{y} = \mathbf{x} + \mathbf{e}$$

  The receiver declares an error if $\mathbf{y}$ is not a codeword
- Any error pattern of weight $d_{min} - 1$ or less will be detected
- Of the $2^n - 1$ nonzero error patterns $2^k - 1$ are the same as nonzero codewords in $C \Rightarrow 2^k - 1$ error patterns are undetectable and $2^n - 2^k$ are detectable
- Let A_i be the number of codewords of weight i in C
- Probability of undetected error over a BSC is given by

$$P_{ue} = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$