Properties of Linear Block Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

July 31, 2015

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 binary 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

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

Example

Find the weight distribution of a linear block with parity check matrix

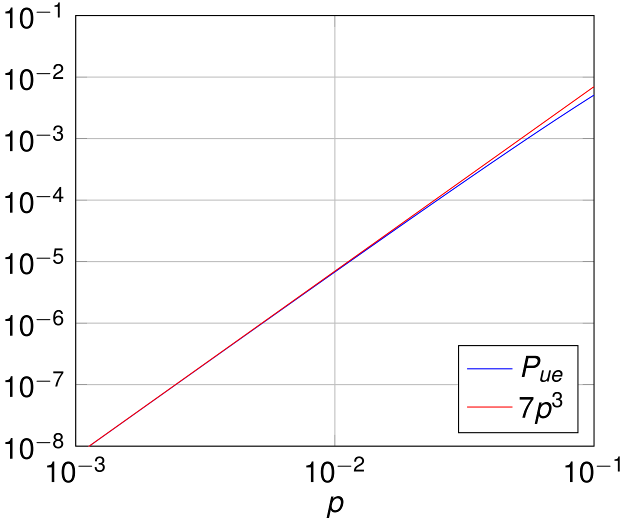
$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$A_0 = 1, A_7 = 1, A_1 = 0, A_2 = 0, A_3 = 7, A_4 = 7, A_5 = 0, A_6 = 0$$

$$P_{ue} = 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7$$

Probability of Undetected Error

$$P_{ue} = 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7$$



The Standard Array

- Let C be an (n, k) linear block code
- Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the codewords in C with $\mathbf{v}_1 = \mathbf{0}$
- The standard array for C is constructed as follows
  1. Put the codewords $\mathbf{v}_i$ in the first row starting with $\mathbf{0}$
  2. Find a smallest weight vector $\mathbf{e} \in \mathbb{F}_2^n$ not already in the array
  3. Put the vectors $\mathbf{e} + \mathbf{v}_i$ in the next row starting with $\mathbf{e}$
  4. Repeat steps 2 and 3 until all vectors in $\mathbb{F}_2^n$ appear in the array
- Example: $G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

0000	1100	0011	1111
1000	0100	1011	0111
0010	1110	0001	1101
0110	1010	0101	1001

Properties of the Standard Array

- Each row has 2^k distinct vectors
- The rows are disjoint
- There are 2^{n-k} rows
- The rows are called cosets of the code C
- The first vector in each row is called a coset leader
- Decoding using the standard array
  - Let $\mathbf{0}, \mathbf{e}_2, \mathbf{e}_3, \ldots, \mathbf{e}_{2^{n-k}}$ be the coset leaders
  - Let D_j be the jth column of the standard array

$$D_j = \{\mathbf{v}_j, \mathbf{e}_2 + \mathbf{v}_j, \mathbf{e}_3 + \mathbf{v}_j, \ldots, \mathbf{e}_{2^{n-k}} + \mathbf{v}_j\}$$

  - Decode a vector which belongs to D_j to $\mathbf{v}_j$
  - Any error pattern equal to a coset leader is correctable
- Every (n, k) linear block code can correct 2^{n-k} error patterns

Example

$$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

000000	011100	101010	110001	110110	101101	011011	000111
100000	111100	001010	010001	010110	001101	111011	100111
010000	001100	111010	100001	100110	111101	001011	010111
001000	010100	100010	111001	111110	100101	010011	001111
000100	011000	101110	110101	110010	101001	011111	000011
000010	011110	101000	110011	110100	101111	011001	000101
000001	011101	101011	110000	110111	101100	011010	000110
100100	111000	001110	010101	010010	001001	111111	100011

- The code has minimum distance 3
- It corrects all single-bit errors and one double-bit error

Syndrome Decoding

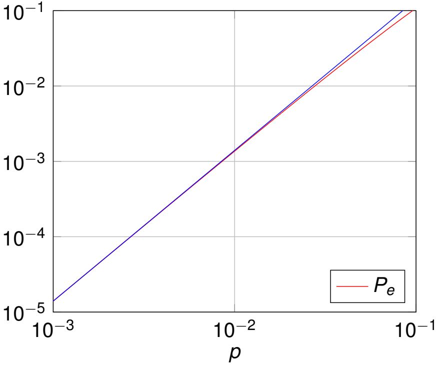
- All vectors in the same row of the standard array have the same syndrome
- Vectors in different rows have different syndromes
- Steps in syndrome decoding
  - Compute the syndrome $\mathbf{y} \cdot H^T$ of the received vector $\mathbf{y}$
  - Find the coset leader $\mathbf{e}_i$ whose syndrome equals $\mathbf{y} \cdot H^T$
  - Decode $\mathbf{y}$ into the codeword $\hat{\mathbf{v}} = \mathbf{y} + \mathbf{e}_i$
- Let α_i be the number of coset leaders of weight i for C
- Probability of decoding error over a BSC is given by

$$P_e = 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}$$

Probability of Decoding Error

$$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$P_e = 1 - (1-p)^6 - 6p(1-p)^5 - p^2(1-p)^4$$



Hamming Bound

Let C be an (n, k) binary linear block code with minimum distance $d_{min} \geq 2t + 1$.

$$2^{n-k} \geq 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}$$

Proof.

Does $d_{min} \geq 2t + 1$ imply that all vectors of weight t or less are coset leaders?

Suppose $\text{wt}(\mathbf{x}) \leq t$ and $\text{wt}(\mathbf{y}) \leq t$. Can $\mathbf{x}$ and $\mathbf{y}$ be in the same coset?

MacWilliams Identity

- Let C be an (n, k) binary linear block code
- Let $A_0, A_1, \ldots, A_n$ be the weight distribution of C
- Let $B_0, B_1, \ldots, B_n$ be the weight distribution of $C^\perp$
- The corresponding weight enumerators are given by

$$
\begin{aligned}
A(z) &= A_0 + A_1 z + \cdots A_n z^n \\
B(z) &= B_0 + B_1 z + \cdots B_n z^n
\end{aligned}
$$

- The MacWilliams identity states that

$$A(z) = 2^{-(n-k)}(1+z)^n B\left(\frac{1-z}{1+z}\right)$$

Example

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

$$\begin{aligned} A(z) &= 1 + 7z^3 + 7z^4 + z^7 \\ B(z) &= 1 + 7z^4 \\ 2^{-3}(1+z)^7 B\left(\frac{1-z}{1+z}\right) &= 2^{-3}(1+z)^7 \left[1 + 7\left(\frac{1-z}{1+z}\right)^4\right] \end{aligned}$$

P_{ue} and $A(z)$

Probability of undetected error over a BSC is given by

$$\begin{aligned}
P_{ue} &= \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} \\
&= (1-p)^n \sum_{i=1}^{n} A_i \left(\frac{p}{1-p}\right)^i \\
&= (1-p)^n \left[-1 + \sum_{i=0}^{n} A_i \left(\frac{p}{1-p}\right)^i\right] \\
&= (1-p)^n \left[A\left(\frac{p}{1-p}\right) - 1\right]
\end{aligned}$$

Questions?