Examples of Linear Block Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

August 18, 2014

Hamming Code

Hamming Code

- For any integer $m \geq 3$, the code with parity check matrix consisting of all nonzero columns of length m is a Hamming code
- For $m = 3$

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

- For $m = 4$

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

- Length of the code $n = 2^m - 1$
- Dimension of the code $k = 2^m - m - 1$
- Minimum distance of the code $d_{min} = 3$

Hamming's Approach

- Observes that a single parity check can detect a single error
- In a block of n bits, m locations are information bits and the remaining $n - m$ bits are check bits
- The check bits enforce even parity on subsets of the information bits
- In the received block of n bits the check bits are recalculated
- If the observed and recalculated values agree write a 0. Otherwise write a 1
- The sequence of $n - m$ 1's and 0's is called the checking number and gives the location of the single error
- To be able to locate all single bit error locations

$$2^{n-m} \geq n + 1 \implies 2^m \leq \frac{2^n}{n+1}$$

Hamming's Approach

- The LSB of the checking number should enforce even parity on locations $1, 3, 5, 7, 9, \ldots$
- The next significant bit should enforce even parity on locations $2, 3, 6, 7, 10, \ldots$
- The third significant bit should enforce even parity on locations $4, 5, 6, 7, 12, \ldots$
- For $n = 7$, the bound on m is

$$2^m \leq \frac{2^7}{7+1} = 2^4$$

- Choose $1, 2, 4$ as parity check locations and $3, 5, 6, 7$ as information bit locations

Exercises

Let $\mathbf{H}$ be a parity check matrix for a Hamming code.

- What happens if we add a row of all ones to $\mathbf{H}$?

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

- What happens if we delete all columns of even weight from $\mathbf{H}$?

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

Reed-Muller Code

Reed-Muller Code

- Let $f(X_1, X_2, \ldots, X_m)$ be a Boolean function of m variables
- For the 2^m inputs the values of f form a vector $\mathbf{v}(f) \in \mathbb{F}_2^{2^m}$
- Example: $m = 3$ and $f(X_1, X_2, X_3) = X_1 X_2 + X_3$

$$\mathbf{v}(f) = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

- Let $P(r, m)$ be the set of all Boolean functions of m variables having degree r or less
- The rth order binary Reed-Muller code $\text{RM}(r, m)$ is given by the vectors

$$\left\{ \mathbf{v}(f) \middle| f \in P(r, m) \right\}$$

- Is $\text{RM}(r, m)$ linear?
- Length of the code $n = 2^m$
- Dimension of the code $k = 1 + \binom{m}{1} + \cdots + \binom{m}{r}$

Basis for RM(2, 4)

$$\mathrm{RM}(2,4) = \left\{ \mathbf{v}(f) \middle| f \in P(2,4) \right\}$$

$$P(2,4) = \langle 1, X_1, X_2, X_3, X_4, X_1X_2, X_1X_3, X_1X_4, X_2X_3, X_2X_4, X_3X_4 \rangle$$

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

Minimum Distance of RM(r, m)

- $\mathrm{RM}(r,m) = \left\{ \mathbf{v}(f) \,\middle|\, f \in P(r,m) \right\}$
- $X_1 X_2 \cdots X_r \in P(r,m) \implies d_{min} \leq 2^{m-r}$
- Let $f(X_1, \dots, X_m)$ be a non-zero polynomial of degree at most r

$$f(X_1, \dots, X_m) = X_1 X_2 \cdots X_s + g(X_1, \dots, X_m)$$

  where $X_1 X_2 \cdots X_s$ is a maximum degree term in f and $s \leq r$
- For any assignment of values to variables $X_{s+1}, \dots, X_m$ in f the result is a non-zero polynomial
- For every assignment of values to $X_{s+1}, \dots, X_m$, there is an assignment of values to $X_1, \dots, X_s$ where f is non-zero $\implies d_{min} \geq 2^{m-s} \geq 2^{m-r}$

$$d_{min} = 2^{m-r}$$

Questions? Takeaways?