Examples of Linear Block Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

August 11, 2015

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, k locations are information bits and the remaining $n-k$ 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 $n-k$ 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

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

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 k is

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

- 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 $\mathrm{RM}(r, m)$ is given by the vectors

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

- Is $\mathrm{RM}(r, m)$ 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)

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

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

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

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

Example

$$f_1(X_1, X_2, X_3, X_4) = X_1 X_2, \quad f_2(X_1, X_2, X_3, X_4) = X_1 X_2 + X_2 X_3 + X_3 X_4 + X_1 + X_3$$

X_1	X_2	X_3	X_4	$f_1(X_1, X_2, X_3, X_4)$	$f_2(X_1, X_2, X_3, X_4)$
0	0	0	0	0	0
0	1	0	0	0	0
1	0	0	0	0	1
1	1	0	0	1	0
0	0	0	1	0	0
0	1	0	1	0	0
1	0	0	1	0	1
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	0	0	0
1	0	1	0	0	0
1	1	1	0	1	0
0	0	1	1	0	0
0	1	1	1	0	1
1	0	1	1	0	1
1	1	1	1	1	1

Decoding the RM(2, 4) Code

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \\ \mathbf{g}_3 \\ \mathbf{g}_4 \\ \mathbf{g}_5 \\ \mathbf{g}_6 \\ \mathbf{g}_7 \\ \mathbf{g}_8 \\ \mathbf{g}_9 \\ \mathbf{g}_{10} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A codeword $\mathbf{v}$ can be expressed as a linear combination of rows of G

$$\mathbf{v} = \begin{bmatrix} v_0 & v_1 & \cdots & v_{14} & v_{15} \end{bmatrix} = \sum_{i=0}^{10} u_i \mathbf{g}_i$$

where u_i's represent message bits

Decoding u_{10}

$$u_{10} = v_0 + v_1 + v_2 + v_3$$
$$u_{10} = v_4 + v_5 + v_6 + v_7$$
$$u_{10} = v_8 + v_9 + v_{10} + v_{11}$$
$$u_{10} = v_{12} + v_{13} + v_{14} + v_{15}$$

Let $\mathbf{r} = \mathbf{v} + \mathbf{e}$ be the received vector.
If $\mathrm{wt}(\mathbf{e}) = 1$, then the following sums have majority equal to u_{10}

$$A_1 = r_0 + r_1 + r_2 + r_3$$
$$A_2 = r_4 + r_5 + r_6 + r_7$$
$$A_3 = r_8 + r_9 + r_{10} + r_{11}$$
$$A_4 = r_{12} + r_{13} + r_{14} + r_{15}$$

Decoding u_9

$$u_9 = v_0 + v_1 + v_4 + v_5$$
$$u_9 = v_2 + v_3 + v_6 + v_7$$
$$u_9 = v_8 + v_9 + v_{12} + v_{13}$$
$$u_9 = v_{10} + v_{11} + v_{14} + v_{15}$$

If $\mathrm{wt}(\mathbf{e}) = 1$, then the following sums have majority equal to u_9

$$A_1 = r_0 + r_1 + r_4 + r_5$$
$$A_2 = r_2 + r_3 + r_6 + r_7$$
$$A_3 = r_8 + r_9 + r_{12} + r_{13}$$
$$A_4 = r_{10} + r_{11} + r_{14} + r_{15}$$

Decoding u_4

After decoding $u_{10}, u_9, u_8, u_7, u_6, u_5$ remove the corresponding basis vectors from $\mathbf{r}$

$$\mathbf{r}^{(1)} = \mathbf{r} + \sum_{i=5}^{10} u_i \mathbf{g}_i = \sum_{i=0}^{4} u_i \mathbf{g}_i + \mathbf{e}$$

If $\mathrm{wt}(\mathbf{e}) = 1$, then the following sums have majority equal to u_4

$$\begin{aligned} A_1 &= r_0^{(1)} + r_1^{(1)}, & A_5 &= r_8^{(1)} + r_9^{(1)} \\ A_2 &= r_2^{(1)} + r_3^{(1)}, & A_6 &= r_{10}^{(1)} + r_{11}^{(1)} \\ A_3 &= r_4^{(1)} + r_5^{(1)}, & A_7 &= r_{12}^{(1)} + r_{13}^{(1)} \\ A_4 &= r_6^{(1)} + r_7^{(1)}, & A_8 &= r_{14}^{(1)} + r_{15}^{(1)} \end{aligned}$$

u_1, u_2, u_3 can also be decoded using eight sums

Decoding u_0

After decoding $u_1, \ldots, u_{10}$ remove the corresponding basis vectors from $\mathbf{r}$

$$\mathbf{r}^{(2)} = \mathbf{r} + \sum_{i=1}^{10} u_i \mathbf{g}_i = u_0 \mathbf{g}_0 + \mathbf{e}$$

There are 16 noisy versions of u_0 whose majority is u_0 if $\mathrm{wt}(\mathbf{e}) = 1$.
This technique is called majority-logic decoding.

Questions?