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* ≥ 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
- 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

$$2^{n-k} \ge n+1 \implies 2^k \le \frac{2^n}{n+1}$$

Hamming's Approach

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

$$2^k \le rac{2^7}{7+1} = 2^4$$

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

Exercises

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

• What happens if we add a row of all ones to H?

• What happens if we delete all columns of even weight from **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 $f(X_1, X_2, ..., X_m)$ 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 $f(X_1, X_2, X_3) = X_1X_2 + X_3$

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

- Let *P*(*r*, *m*) be the set of all Boolean functions of *m* variables having degree *r* or less
- The *r*th order binary Reed-Muller code RM(*r*, *m*) is given by the vectors

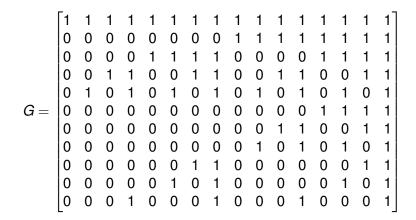
$$\left\{\mathbf{v}(f)\middle|f\in P(r,m)\right\}$$

- Is 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)

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

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



Minimum Distance of RM(r, m)

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

- $X_1 X_2 \cdots X_r \in \mathcal{P}(r,m) \implies d_{min} \leq 2^{m-r}$
- Let f(X₁,..., X_m) be a non-zero polynomial of degree at most r

$$f(X_1,\ldots,X_m)=X_1X_2\cdots X_s+g(X_1,\ldots,X_m)$$

where $X_1 X_2 \cdots X_s$ is a maximum degree term in f and $s \leq r$

- For any assignment of values to variables X_{s+1},..., X_m in f the result is a non-zero polynomial
- For every assignment of values to X_{s+1},..., X_m, there is an assignment of values to X₁,..., X_s where *f* is non-zero ⇒ d_{min} ≥ 2^{m-s} ≥ 2^{m-r}

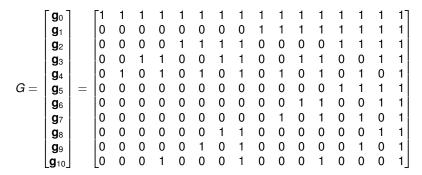
$$d_{min} = 2^{m-r}$$

Example

 $f_1(X_1, X_2, X_3, X_4) = X_1X_2, \ f_2(X_1, X_2, X_3, X_4) = X_1X_2 + X_2X_3 + X_3X_4 + X_1 + X_2X_4 + X_2X_4 + X_1 + X_2X_4 + X_2X_4 + X_1 + X_2X_4 + X_1 + X_2X_4 +$

<i>X</i> ₁	<i>X</i> ₂	<i>X</i> ₃	<i>X</i> 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



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 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 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 **r**

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

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

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

 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 **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 wt(\mathbf{e}) = 1. This technique is called majority-logic decoding.

Questions?