E2 205 Error-Control Coding
Lecture 11

Scribe - Puja Parmar

September 18, 2019

1 Boolean function

Definition 1 *Any function defined on $\mathbb{F}_2^n$, taking values either 0 or 1 is called a Boolean function.*

$$f : \mathbb{F}_2^n \to \mathbb{F}_2$$

1.1 Lagrange Interpolation

$$f(x_1, \ldots, x_m) = \sum_{a_1 \cdots a_m} f(a_1 \cdots a_m) \prod_{i=1}^{m} (x_i + a_i + 1)$$

Thus every Boolean function can be represented as a multi variable (MV) polynomial of degree $\leq m$.

$$f(x_1, \ldots, x_m) = a_0 + \sum_{i=1}^{m} a_i x_i + \sum_{\substack{i,j=1 \\ j>i}}^{m} a_{ij} x_i x_j + \cdots + a_{1 \cdots m} x_1 x_2 \cdots x_m$$

Lagrange interpolation establishes a map from Boolean function over $\mathbb{F}_2^m$ to a multi variable polynomial in m binary variables $X_1, \ldots, X_m$. The set of all Boolean functions over $\mathbb{F}_2^m$ is a vector space of dimension 2^m. On the other hand, the monomials 1, $\{x_i\}_{i=1}^m$, $\{x_i x_j\}_{1 \leq i < j \leq m}$, $\ldots$, $x_1 \ldots x_m$ span this space.
(Note that the map from Boolean function to multivariate polynomial is linear)

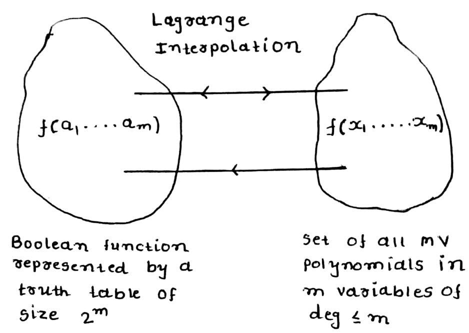

Figure 1: Mapping from Boolean function to MV polynomial

Thus the monomials form a basis for the set of all multivariate polynomials. The corresponding Boolean functions form a basis for the space of all Boolean functions.
Note that

$$\sum_{x_1\cdots x_m} f(x_1\cdots x_m) = a_{1\cdots\ m}$$

This is because

$$\sum_{\substack{x_1\cdots x_m\\ \in\mathbb{F}_2^m}} x_{i_1}x_{i_2}\cdots x_{i_r} = \sum_{x_{i_1}}\sum_{x_{i_2}}\cdots\sum_{x_{i_r}} x_{i_1}x_{i_2}\cdots x_{i_r}\sum_{x_j, j\notin\{i_1\ldots i_r\}} 1$$

$$= \begin{cases} 2^{m-r} = 0 \pmod 2 & \text{if } 0 \le r \le m-1 \\ 1 & \text{if } m = r \end{cases}$$

$$\begin{aligned}\text{Number of monomials in m binary variables} &= 1 + m + \binom{m}{2} + \cdots + \binom{m}{m} \\ &= 2^m\end{aligned}$$

2 Reed Muller(binary) codes

Definition 2 *The r^{th} order Reed Muller code RM(r,m) is given by:*
$RM(r,m) = \left\{ \left(f(\underline{a}), \underline{a} \in \mathbb{F}_2^n \right) \mid deg(f) \le r \right\}$

length of RM(r,m) $= 2^m$

dimension of RM(r,m) $= \sum_{i=0}^{r} \binom{m}{i}$

Example 1 *RM(2,4)*
length $= 2^4$
dimension $= \binom{4}{0} + \binom{4}{1} + \binom{4}{2} = 11$

$$f(x_1, x_2, x_3, x_4) = a_0 + \sum_{i=1}^{4} a_i x_i + \sum_{i=1}^{4} \sum_{j=1}^{4} a_{i_j} x_i x_j$$

Theorem 1 $\big(RM(r,m)\big)^{\perp} = RM(m-r-1,m)$

Proof :

$$\text{Note: } \sum_{i=0}^{m-r-1} \binom{m}{i} = \sum_{j=r+1}^{m} \binom{m}{j}$$

$$\text{and } \sum_{i=0}^{m-r-1} \binom{m}{i} + \sum_{i=0}^{r} \binom{m}{i} = 2^m \tag{1}$$

$$\begin{aligned} \text{Let, } & f(x_1, \ldots, x_m) \quad \text{have degree} \le r \\ & g(x_1, \ldots, x_m) \quad \text{have degree} \le m-r-1 \end{aligned}$$

$$\begin{aligned} \text{Then } & \big(f(\underline{a}), \underline{a} \in \mathbb{F}_2^n\big) \in RM(r,m) \\ & \big(g(\underline{a}), \underline{a} \in \mathbb{F}_2^n\big) \in RM(m-r-1,m) \end{aligned}$$

$$\text{Consider, } \sum_{\substack{x_1 \cdots x_m \\ \in \mathbb{F}_2^n}} f(x_1, \ldots, x_m) \quad g(x_1, \ldots, x_m) = 0$$

degree $\le m-r-1+r = m-1$ because $\sum_{\underline{x} \in \mathbb{F}_2^n} h(x_1, \ldots, x_m) = 0$ for any Boolean function of degree <m (since the coefficient $a_{12\ldots m} = 0$)

Thus $\quad RM(m-r-1,m) \subseteq \big(RM(r,m)\big)^{\perp}$

$$\text{But, } dim\big(RM(m-r-1,m)\big) = \sum_{i=0}^{m-r-1} \binom{m}{i}$$
$$= 2^m - \sum_{i=0}^{r} \binom{m}{i} \quad \text{(from equation 1)}$$

$\therefore \big(RM(r,m)\big)^{\perp} = RM(m-r-1,m)$

Example 2 $\big(RM(2,4)\big)^{\perp} = RM(1,4)$

2.1 Minimum Distance of RM(r,m)

Theorem 2 $d_{min}\big(RM(r,m)\big) = 2^{m-r}$

Proof :
Since we are able to correct $t = 2^{m-r-1} - 1$ errors

$$d_{min} \geq 2(2^{m-r-1} - 1) + 1$$
$$= 2^{m-r} - 1$$

But the hamming weight of every code word in RM(r,m) is even for r<m

$$\therefore d_{min} \geq 2^{m-r}$$

But the code word associated to $X_1X_2 \ldots X_r$ has hamming weight $= 2^{m-r}$

$$\therefore d_{min} = 2^{m-r} \quad (\text{since } d_{min} = w_{min})$$

For the case $r = m$, RM(m,m) = set of all 2^m tuples.

$$\therefore d_{min} = 1$$
$$= 2^{m-r} \quad \text{in this case as well}$$

Example 3 *Consider RM(*$2,4$*)*
$[n,k,d] = [16,11,4]$
$f(x) = 1 + x_1 + x_2 + x_1x_2 + x_3x_4$
Truth table for $f(x)$ *is shown in fig:2*

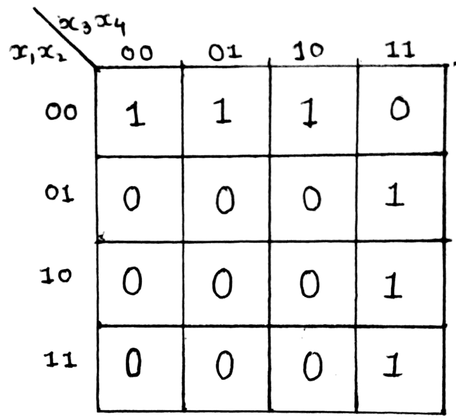

Figure 2: A Boolean function in 4 variables

$f(x_1, x_2, x_3, x_4) = a_0 + \sum_{i=1}^{4} a_i x_i + \sum_{j>i} a_{ij} x_i x_j$
to find a_{34} *we set* $x_1 = \theta_1,\ x_2 = \theta_2 \quad \theta_1, \theta_2 \in \mathbb{F}_2$
By majority logic decoding

$$\hat{a}_{34} = \sum_{x_3 x_4} f(\theta_1, \theta_2, x_3, x_4) = 1$$

same way, by majority logic decoding

$$\hat{a}_{12} = \sum_{x_1 x_2} f(x_1, x_2, \theta_3, \theta_4) = 1$$

Example 4 *Consider* $g(x_1 x_2 x_3 x_4) = f(x_1 x_2 x_3 x_4) + x_1 x_2 + x_3 x_4$ *where* $f(x_1 x_2 x_3 x_4)$ *is from example 3.Truth table for* $g(x)$ *is shown in fig:3.*
$g(x_1 x_2 x_3 x_4) = a_0 + a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4$

$x_1x_2 \backslash x_3x_4$	00	01	10	11
00	1	1	1	1
01	0	0	0	0
10	0	0	0	0
11	1	1	1	1

Figure 3: A Boolean function in 4 variables

By majority logic decoding,

$$\hat{a}_4 = \sum_{x_4} g(\theta_1, \theta_2, \theta_3, x_4) = 0 \quad \theta_1, \theta_2, \theta_3 \in \mathbb{F}_2^m$$