| | |
|---|---|
| **Topics in Coding Theory** | Date - 3-3-2021 |
| Lecture 11 | |
| *Instructor: Dr. Prasad Krishnan* | *Scribe: Rasagna Chigullapally(20171003)* |

# 1 Reed-Muller Codes

We have already discussed Reed-Solomon codes which are single variable evaluation codes.(m(X) of deg≤k-1 over $\mathbb{F}_q$ - evaluate at some distinct points of $\mathbb{F}_q$ to get codeword corresponding to m(X))

**Generalized Reed-Muller Codes:** These are evaluation based codes with multivariate polynomials for message $M(X_1, X_2, ...X_m)$ under some degree constraint(s).(These are evaluated at points from $\mathbb{F}_q$ to get components of the codeword)
Discussion here is based on **Binary Reed-Muller codes**(under the total degree constraint).
Note that for any $\alpha$ in $\mathbb{F}_2$, $\alpha^2 = \alpha$.

## 1.1 Binary Reed Muller Codes

Set of message polynomials for RM code RM(m,r)

$$\mathcal{M} = \{M(X_1, X_2, .., X_m) = \sum_{(i_1,..,i_m)\in\{0,1\}^m : \sum_{j=1}^m i_j \leq r} a_{i_1,..,i_m} X_1^{i_1} X_2^{i_2} .. X_m^{i_m} : a_{i_1,..,i_m} \in \mathbb{F}_2\}$$

RM(m,r) code is defined as -
Codeword corresponding to message polynomial $M(X_1, .., X_m) = (M(X_1, .., X_m)|_{(X_1,..,X_m)\in\mathbb{F}_2^m})$ is of length $2^m = n$ (Coordinates of the codeword are indexed by the vector form $\mathbb{F}_2^m$).

$$RM(m, r)code = \{(M(X_1, .., X_m)|_{(X_1,..,X_m)\in\mathbb{F}_2^m}) : M(X_1, .., X_m) \in \mathcal{M}\}$$

**Size of code** = Number of message polynomials($|\mathcal{M}|$) = $2^{\sum_{j=0}^{r}\binom{m}{j}}$ (because any $0 \leq j \leq r$ variables of the m variables can be a monomial)

**Example 1.** *RM(m=4,r=2)*
$\mathcal{M} = \{M(X_1, X_2, .., X_m) = a_{1100}X_1X_2 + a_{1010}X_1X_3 + a_{1001}X_1X_4 + a_{0110}X_2X_3 + a_{0101}X_2X_4 + a_{0011}X_3X_4 + a_{1000}X_1 + a_0 100X_2 + a_{0010}X_3 + a_{0001}X_4 + a_{0000} : a_{i_1,i_2,i_3,i_4} \in \mathbb{F}_2\}$

*Eg of message polynomial -*

- $M(X_1, .., X_m) = X_1X_2 + X_3$
- $M(X_1, .., X_m) = 1$
- $M(X_1, .., X_m) = X_1 + X_2 + 1$

*Codeword corresponding to* $(X_1X_2 + X_3) = (0_{(X_1X_2X_3X_4=0000)}, 0_{(1000)}, 1_{(1100)}, ..)$ *- 16 length*
*size of the code* $= 2^{11} = 2^{\sum_{j=0}^{2}\binom{4}{j}}$

**Claim:** This is a **linear code**.($\alpha\underline{c}_1 + \underline{c}_2 \in \mathcal{C}$ $\forall \underline{c}_1, \underline{c}_2 \in \mathcal{C}, \forall\alpha \in \mathbb{F}_q$, since $\mathbb{F}_q = \mathbb{F}_2$, we only have to check sum of codewords is a codeword or not)

*Proof.* Let $\underline{c}_1, \underline{c}_2 \in \mathcal{C} = RM(m,r)$
Then $\underline{c}_1 + \underline{c}_2 \in \mathcal{C}$ (why?)
since $\underline{c}_1, \underline{c}_2 \in \mathcal{C}$, $\exists\ M_1, M_2 \in \mathcal{M}$ such that

$$\underline{c}_1 = (M_1(X_1,..,X_m)|_{(X_1,..,X_m)\in\mathbb{F}_2^m}), \underline{c}_2 = \{(M_2(X_1,..,X_m)|_{(X_1,..,X_m)\in\mathbb{F}_2^m})$$

Then

$$\underline{c}_1 + \underline{c}_2 = (M_3(X_1,..,X_m)|_{(X_1,..,X_m)\in\mathbb{F}_2^m})$$

where $M_3 = M_1 + M_2$(sum of polynomials).
But $M_3(X_1,..,X_m)$ obeys the same degree constraints as $M_1, M_2$ and hence $M_3 \in \mathcal{M}$(valid message polynomial).
$\implies \underline{c}_1 + \underline{c}_2$ is the evaluation of a valid message polynomial $\implies \underline{c}_1 + \underline{c}_2 \in \mathcal{C}$. $\square$

**Dimension** of RM(m,r)=$\log_2 |\mathcal{C}| = \sum_{j=0}^{r} \binom{m}{j} = k$ (no.of coefficients appearing in an arbitrary msg polynomial in $\mathcal{M}$)
**length of code** n $= 2^m =$ no. of evaluations.
**Rate** $= \dfrac{k}{n} = \dfrac{\sum_{j=0}^{r} \binom{m}{j}}{2^m}$

what about minimum distance?
**Claim:** $d_{min}(RM(m,r)) = 2^{m-r}$

*Proof.* Since RM(m,r) is a linear code $d_{min} =$ minimum wt of non-zero codewords, Non-zero codewords correspond to evaluations of non-zero message polynomials.
Let $M(X_1,..,X_m)$ be an arbitrary non-zero polynomial.

In any non-zero msg polynomial, degree(monomial) $\leq$ r. Assume that the max degree of any monomial in $M(X_1,..,X_m)$ is equal to l.
without loss of generality, let this be $X_1X_2..X_l$
Thus $M(X_1,..,X_m) = X_1X_2..X_l + M^1(X_1,..,X_m)$ for some polynomial $M^1$.
Now in the above, let $(X_{l+1},..X_m) = (0,..,0)$
$\implies M(X_1,..,X_l,X_{l+1}=0,..,X_m=0) = X_1X_2..X_l +$ some terms in $(X_1,X_2,..,X_l) =$ non-zero polynomial

Since this is a non-zero polynomial in $(X_1,..,X_l)$, atleast one evaluation of this polynomial will be non-zero.(Proof is continued in next class) $\square$