Class 19 :

$$\underline{y} = (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) \quad 2^m \text{ length.}$$

Suppose we look at those coordinate positions of y, indexed by all vectors $\underline{x} \in \mathbb{F}_2^m$ such that $x_{r+1} = \cdots = x_m = 0$.

Let us label these 2^r coordinate positions as $\mathbb{B}$.

$$\mathbb{B} = \{ \underline{x} \in \mathbb{F}_2^m : x_{r+1} = \cdots = x_m = 0 \} \subset \mathbb{F}_2^m.$$

Note that $\mathbb{B}$ is a subspace of dim $m-r$.

Following Reed's ML algo:

Define $y_{/\mathbb{B}}(\mathbb{B}) = \bigoplus_{\underline{x} \in \mathbb{B}} y(\underline{x})$

Consider

$$T = \left\{ \underline{x} \in \mathbb{F}_2^m : (x_{r+1}, \dots, x_m) = \underline{a}_{1 \times m-r} \right\}$$

Define $y_{/\mathbb{B}}(T) = \bigoplus_{\underline{x} \in T} y(\underline{x})$

But is T a subspace? If and only if $\underline{a} = 0$

But $T = \{ (\underline{0}, \underline{a}) + \underline{x} : \underline{x} \in \mathbb{B} \} \rightarrow$ coset of subspace $\mathbb{B}$

Generalizations

(We define this for any subspace $\mathbb{B}$ of $\mathbb{F}_2^m$ of dim $s \leq r$).

For the subspace $\mathbb{B}$, we can obtain any coset of $\mathbb{B}$, by choose some $\underline{x}_1 \notin \mathbb{B}$, & define

$$T_{\underline{x}_1} = \{ \underline{x}_1 + \underline{x} : \underline{x} \in \mathbb{B} \}.$$

Easy to show that

$$|T_{\underline{x}_1}| = |\mathbb{B}|$$

We are now discussing general scenario.

How many such distinct cosets are possible for a $\dim(s)$ subspace $\mathbb{B}$ of $\mathbb{F}_2^m$?

Claim 1: $T_{x_1} \cap T_{x_2} = \begin{cases} \phi & \text{if } x_1 \notin T_{x_2} \\ T_{x_1} & \text{otherwise} \end{cases}$

Proof:

If $x_1 \notin T_{x_2}$ then we will prove $T_{x_1} \cap T_{x_2} = \phi$.

We do proof by contra. Suppose $T_{x_1} \cap T_{x_2} \neq \phi$ (ie)

$\underline{t} \in T_{x_1} \cap T_{x_2}$.

Then we can write $\underline{t} = \underline{x_1} + \underline{x}$, where $\underline{x} \in \mathbb{B}$

$= \underline{x_2} + \underline{x'}$, where $\underline{x'} \in \mathbb{B}$

Then $x_1 + \underline{x} = x_2 + \underline{x'} \Rightarrow x_1 = x_2 + (\underline{x} + \underline{x'}) \in T_{x_2}$ since $\underline{x} + \underline{x'} \in \mathbb{B}$ as $\mathbb{B}$ is subspace

$\Rightarrow$ So we have a contradiction with given statement that $x_1 \notin T_{x_2}$.

Now we take the second subclaim:

Gn: $x_1 \in T_{x_2}$

Tp: $T_{x_1} \cap T_{x_2} = T_{x_1}$

Proof: By contradiction: Suppose to the contrary, suppose some $x_1' \in T_{x_1} \setminus T_{x_2}$ exists. [assumption]

$x_1' = \underline{x_1} + \underline{x}$, for some $\underline{x} \in \mathbb{B}$.

Applying given statement, as $x_1 \in T_{x_2}$,

$x_1' = x_2 + (\underline{x}' + \underline{x})$, for some $x' \in \mathbb{B} \Rightarrow x_1' \in T_{x_2}$

$\in \mathbb{B}$ as $\mathbb{B}$ is a subspace

Which is a contradiction with assumption.

(Concludes the claim)

It is also very easy to show every vector in $\mathbb{F}_2^m$ is in some coset.

↳ Claim 2.

By Claim 1 & Claim 2, the set of distinct cosets of $\mathbb{B}$ in $\mathbb{F}_2^m$ partition $\mathbb{F}_2^m$.

$$\Rightarrow \text{The no of such cosets is } \frac{|\mathbb{F}_2^m|}{|\mathbb{B}|} = 2^{m-s}$$

How to get the cosets?

$$\mathbb{F}_2^m/\mathbb{B} = \left\{ T_{\underline{x}_0=\underline{0}} = \mathbb{B},\ T_{\underline{x}_1},\ T_{\underline{x}_2}, \ldots, T_{x_{2^{m-s}-1}} \right\}$$

↓pick x_1 not in $\mathbb{B}$

pick $x_2 \in \mathbb{F}_2^m \setminus T_{x_1} \cup T_{x_0}$ . . .

pick $x_{2^{m-s}-1}$ ∉ all prior cosets.

These cosets partition $\mathbb{F}_2^m$

Recall

$$y_{/\mathbb{B}}(T) = \bigoplus_{\underline{x} \in T} y(\underline{x})$$

(this is 1 bit, resulting from sum of all the $|T| = 2^8$ components $y(\underline{x})$ of y corresponding to $\underline{x} \in T$)

$$\underline{y_{/\mathbb{B}}} = \left(y_{/\mathbb{B}}(T) : T \in \boxed{\mathbb{F}_2^m / \mathbb{B}} \right)$$

vector of length 2^{m-8}

$\underline{\in \mathbb{F}_2^{m-8}}$

quotient space of subspace $\mathbb{B}$.

Lemma: Suppose $\underline{c} \in RM(m, r)$. Let B be a s-dim subspace of $\mathbb{F}_2^m$ where $s \leq r$. Then

$$\underline{c_{/B}} = \left(c_{/B}(T) : T \in \mathbb{F}_2^m / B \right)$$

is a codeword of $RM(m-s, r-s)$.

Example (before discussing the proof):

Suppose $m = 4$, $r = 2$. Let the msg poly corresponding to $\underline{c} \in RM(4,2)$ be $M(X_1, X_2, X_3, X_4) =$

$$X_1 X_2 + X_1 + X_3 + X_4 + 1$$

Now, let us take a subspace of dimension $\mathbb{B}$ of dim 2,

$$\mathbb{B}^{\perp} = \left\{ \underline{x} \in \mathbb{F}_2^4 : \begin{array}{l} x_1 + x_2 = 0 \\ x_2 + x_3 = 0 \\ x_3 + x_4 = 0 \end{array} \right\}$$

$\Rightarrow x_2 = x_1$

$\Rightarrow x_3 = x_2$

$\Rightarrow x_4 = x_3$.

$\Rightarrow \underline{x_1 = x_2 = x_3 = x_4}$

$X_1 = X_2 = X_3 = X_4$

3 constants

plug in

$M(x_1, \ldots, x_4)$

$\tilde{M}(\quad = M(X_1 \ldots X_4) \Big|_{\text{plug 3 constants}} = X_1^2 + X_1 + X_1 + X_1 + 1$

$= X_1 + X_1 + 1$ (since in $\mathbb{F}_q$ $\underline{X^q = X}$).

in $\mathbb{F}_2$ $X^2 = X$

$\tilde{M}(X_1) = 1$

Exercise. Verify that $\underline{C}_{\mathbb{B}}$ = Evaluation vector of $\tilde{M}(\_\_)$ $\longrightarrow$ To be corrected in next class.