Class 14

We saw defn of the <u>dual</u> code of a linear code $\mathcal{C}$ in the quiz.

<u>Defn:</u> Let $\mathcal{C}$ be a $[n,k]$ linear code over $\mathbb{F}_q$.

Then $\mathcal{C}^{\perp}$ (perp) $= \{ \underset{\text{(row vector)}}{\underline{v}} \in \mathbb{F}_q^n : \underset{\text{row}}{\underline{v}}\, \underset{\text{column}}{\underline{c}^T} = 0 \ \forall\, \underline{c} \in \mathcal{C} \}$

$\underline{v}\,\underline{c}^T \in \mathbb{F}_q$

(this is a dot product)
but not inner product.

This is not an '<u>inner product</u>' as you might studied in std L. Alg course.

$\downarrow$

$$\boxed{\text{In an inner product defn, } \langle \underline{v}, \underline{v} \rangle = 0, \text{ then } \underline{v} = \underline{0}}$$

But here that will not always be true. For example, say $\underline{v} \in \mathbb{F}_2^n$ is even weighted vector. Then $\underline{v}^T \underline{v} = 0 \pmod 2$

$\in \mathbb{F}_2$ operation

but $\underline{v}$ need not be zero vector.

$$\left.\begin{array}{l} \underline{\dim(\mathcal{C}^\perp) = n-k} \\ \mathcal{C}^\perp \text{ is linear} \end{array}\right\} \Rightarrow \quad \mathcal{C}^\perp \text{ is an } [n, n-k] \text{ linear code.}$$

Easy to show

Duality Result for RM codes:

Claim: Let $\mathcal{C} := RM(m, r)$. Then $\mathcal{C}^{\perp} = RM(m, m-r-1)$

Proof: Let $\underline{v} \in RM(m, m-r-1)$ be an arbitrary codeword. Then there exists some msg poly $M_2(X_1, \ldots, X_m)$ such that $\deg(M_2) \le m-r-1$ &

$$\underline{v} = \left(M_2(X_1, \ldots, X_m) \Big|_{(X_1, \ldots X_m) \in \mathbb{F}_2^m} \right).$$

We want to show $\underline{v} \in \mathcal{C}^{\perp}$ (i.e.) $\underline{v}$ is orthogonal to each codeword in $\mathcal{C}$.

Let $\underline{c}$ be an arbitrary codeword in $\mathcal{C} = RM(m, r)$. Then $\exists$ some $M_1(X_1, \ldots X_m)$ such that $(M_1(X_1 \ldots X_m)|_{\mathbb{F}_2^m}) = \underline{c}$

Then clearly $\underline{v}\,\underline{c}^T = \sum_{\underline{a}\in\mathbb{F}_2^m} M_1(x_1 x_2 \ldots x_m)\Big|_{\underline{x}=\underline{a}} \; M_2(x_1 \ldots x_m)\Big|_{\underline{x}=\underline{a}}$

(This add is mod 2 addition)

$$= \sum_{\underline{a}\in\mathbb{F}_2^m} \Big(M_1(x_1 \ldots x_m)\, M_2(x_1, \ldots x_m)\Big)\Big|_{\underline{x}=\underline{a}} \longrightarrow \text{I}$$

Let $M_3(x_1 \ldots x_m) = M_1 M_2$. Then $\deg(M_3) \le (m-r-1) + r$
$\le m-1$

Now the vector $\underline{y} = \Big(M_3(x_1 \ldots x_m)\Big|_{\underline{x}\in\mathbb{F}_2^m}\Big) \in \underline{RM(m, m-1)}$.

$\hookrightarrow$ has min distance $= 2$.

Then $w_H(\underline{y}) \longrightarrow$ weight which is even. [Exercise) Pls try!

Using this in I implies the $\underline{v}\,\underline{c}^T = 0 \pmod 2$

Thus every $\underline{v} \in RM(m, m-r-1)$ is orthogonal to $\mathcal{C}$.

$\Rightarrow \quad RM(m, m-r-1) \subseteq \mathcal{C}^{\perp}$. → Step 1 → (PTO)

Now we know that $\dim(\mathcal{C}) + \dim(\mathcal{C}^{\perp}) = n = 2^m$

Now checking

$$\dim(\mathcal{C}) + \dim(RM(m, m-r-1)) = \dim(RM(m, r)) + \dim(RM(m, m-r-1))$$

$$= \sum_{j=0}^{r} \binom{m}{j} + \sum_{j'=0}^{m-r-1} \binom{m}{j'}$$

$$= \sum_{j=0}^{r} \binom{m}{j} + \sum_{j=r+1}^{m} \binom{m}{j} = 2^m.$$

$\Rightarrow \dim(RM(m, m-r-1)) = \dim(\mathcal{C}^{\perp})$ → Step 2 (PTO)

$\Rightarrow RM(m, m-r-1) = \mathcal{C}^{\perp}$. QED.

ASIDE:

General idea to show equality of 2 subspaces of a vector space.

Let U, V be subspaces of v.s W.

We want to check if $U = V$.

__Step 1:__ Show that $U \subseteq V$ by proving every $\underline{u} \in U$ is also lying in $\underline{V}$.

__Step 2:__ Instead of showing $V \subseteq U$, we can show (if that's easier), $\dim(U) = \dim(V)$.

By Step 1 & Step 2 we have proved $U = V$.

Decoding of RM codes (Majority logic decoding - $O(n)$ steps for each coefficient of msg polynomial)

upto half of min distance

[no of correctable errors $= \frac{d(\mathcal{C})-1}{2}$]

[Unique decoding]

$\Rightarrow O(nk)$ total steps.

where $k = \sum_{i=0}^{r} \binom{m}{i}$.

$\Rightarrow O(2^m k)$ steps.

(will clarify this later) unclear

Lemma (needed to see the decoding algo):

Suppose we have a poly over $\mathbb{F}_2$ in l variables, of degree $< l$. (Say $g(x_1, \ldots, x_l)$ & $\deg(g) < l$)

Then $$\sum_{(x_1 \ldots x_\ell) \in \mathbb{F}_2^\ell} g(x_1, \ldots, x_\ell) = 0.$$

Proof: [General Research tip / Paper Reading Tip:

Statements of Theorems (or any claim) with general quantities cannot be proved completely via examples or particular values of the quantities. BUT for understanding the statement or for getting ideas for proof, plug in various values for the quantities REALLY HELPS!].