Lecture : Vector spaces (Contd.) and Linear Codes

Vector Spaces (a Refresher), Contd. :

Recall the definition of a vector space $(V, +, \mathbb{F}, \cdot)$ defined over a (finite) field $\mathbb{F}$. We shall now quickly go over some fundamental vector spaces associated with matrices.

Proposition 1 : Let H be an $m \times n$ matrix over a field $\mathbb{F}$. Then,

$$\mathcal{L} = \{\underline{x} : H\underline{x}^T = \underline{0}\}$$

is a subspace of $\mathbb{F}^n$, denoted as nullspace(H).

Proof : We use the fact we had encountered earlier : it suffices to show that for $\underline{x}_1, \underline{x}_2 \in \mathcal{L}$, we must have $\underline{x}_1 + \alpha \cdot \underline{x}_2 \in \mathcal{L}$, for any $\alpha \in \mathbb{F}$.

This is easy to verify, since $H(\underline{x}_1^T + \alpha \cdot \underline{x}_2^T) = 0$. ☑

Defn: Given vectors $\underline{v}_1, \cdots, \underline{v}_m \in V$, a vector of the form

$$\underline{w} = \alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \cdots + \alpha_m \underline{v}_m,$$

where $\alpha_j \in \mathbb{F}$, $j \in [m]$, is called a "linear combination" of $\underline{v}_1, \cdots, \underline{v}_m$.

HW: Verify that the set

$$W \triangleq \left\{ \sum_{j=1}^{m} \alpha_j \cdot \underline{v}_j \;:\; \alpha_j \in \mathbb{F},\ \forall j \in [m] \right\}$$

is a subspace of V. Such a subspace is denoted as $\text{span}(\underline{v}_1, \dots, \underline{v}_m)$.

Def 2: For a $k \times n$ matrix G over $\mathbb{F}$, with rows $g_1, \dots, g_k$, the vector space $\text{span}(g_1, \dots, g_k)$ is called the "rowspace" of G.

Def 3: Vectors $\underline{v}_1, \dots, \underline{v}_m \in V$ are "linearly independent" (over the field $\mathbb{F}$) if

$$\sum_{j=1}^{m} \alpha_j \cdot \underline{v}_j = 0 \iff \alpha_1 = \alpha_2 = \dots = \alpha_m = 0.$$

The vectors are called "linearly dependent", otherwise.

Example: Given $G = \begin{matrix} g_1 \to \\ g_2 \to \\ g_3 \to \end{matrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$, over $\mathbb{F}_2$, we have that g_1, g_2, g_3 are linearly independent over $\mathbb{R}$, but linearly dependent over $\mathbb{F}_2$.

Hence,

$$\text{span}_{\mathbb{F}_2}(g_1, g_2, g_3) = \text{span}_{\mathbb{F}_2}(g_1, g_2).$$

Def 4: Given a matrix A over a field $\mathbb{F}$,

$$\text{rank}_{\mathbb{F}}(A) = \text{rank}(A) \triangleq \text{max. \# lin. indep. rows of } A$$
$$= \text{max. \# lin. indep. cols. of } A$$
$$= \text{rank}(A^T).$$

Example: The rank can be computed by bringing the matrix A to its "reduced row echelon form" (RREF).

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow[\text{over } \mathbb{F}_2]{\text{RREF}} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \Rightarrow \text{rank}_{\mathbb{F}_2}(A) = 2.$$

later ↑

Def. 5: Given a (finite-dimensional) vector space V over a field $\mathbb{F}$, a set of vectors that is linearly independent over $\mathbb{F}$ and spans V is called a basis of V.

Example: Consider the vector space $\mathbb{F}_d[x]$, consisting of all polynomials of degree $\leq d$ over $\mathbb{F}$.

A basis for this vector space is the collection of monomials

$$\{1, x, x^2, \ldots, x^d\}.$$

FACTS:

① Let $\underline{b}_1, \underline{b}_2, \cdots, \underline{b}_n$ be a basis of a vector space V. Then, any $\underline{v} \in V$ can be expressed uniquely as a linear combination of $\underline{b}_1, \ldots, \underline{b}_n$.

② All bases of a vector space have the same size.

Def 6 (following ② above): The no. of elements in any basis of a vectorspace V over a field $\mathbb{F}$ is called the "dimension of V", denoted by

$$\dim_{\mathbb{F}}(V) \equiv \dim(V).$$

FACT (Rank-Nullity Theorem): Let A be an $m \times n$ matrix over a field $\mathbb{F}$. Then,

$$\text{rank}_{\mathbb{F}}(A) + \text{nullity}_{\mathbb{F}}(A) = n,$$

where $\text{nullity}_{\mathbb{F}}(A) \triangleq \dim(\text{nullspace}(A))$ and $\text{rank}_{\mathbb{F}}(A) = \dim(\text{rowspace}(A))$.

Linear codes

We now get introduced to an important family of structured codes: linear codes. In what follows, we let $\mathbb{F} = \mathbb{F}_q$ to be a finite field with q elements.

Def. 7: A linear code $\mathcal{C}$ over $\mathbb{F}$ is a subspace of $\mathbb{F}^n$, where n is called the "blocklength" of $\mathcal{C}$.

Def 8: An $[n,K,d]_q$ linear code $\mathcal{C}$ is a linear code over $\mathbb{F}_q$ of blocklength n, dimension $\dim(\mathcal{C})=K$, and minimum distance $d_{\min}(\mathcal{C})=d$.

Lemma 2: An $[n,K]_q$ linear code $\mathcal{C}$ has q^K codewords.

Proof: Exercise.

Remark: The rate of an $[n,K]_q$ linear code over $\mathbb{F}_q$ is

$$R = \frac{\log_q(q^K)}{n} = \frac{K}{n}.$$

For a given vector $\underline{x} \in \mathbb{F}_q^n$, let $w(\underline{x}) = w_H(\underline{x}) \triangleq \#$ non-zero coordinates in $\underline{x}$.

"Hamming weight"

Proposition 3: For a linear code $\mathcal{C}$, we have

$$d_{\min}(\mathcal{C}) = \min_{\underline{c} \in \mathcal{C},\, \underline{c} \neq \underline{0}} w_H(\underline{c}).$$

Proof: Note that

$$d_{\min}(\mathcal{C}) = \min_{\underline{c}_1, \underline{c}_2 \in \mathcal{C},\, \underline{c}_1 \neq \underline{c}_2} d_H(\underline{c}_1, \underline{c}_2)$$

$$= \min_{\underline{c}_1, \underline{c}_2 \in \mathcal{C},\, \underline{c}_1 \neq \underline{c}_2} w_H(\underline{c}_1 - \underline{c}_2) \quad \text{(by linearity)} \quad = \min_{\underline{c} \in \mathcal{C},\, \underline{c} \neq \underline{0}} w_H(\underline{c}). \qquad \blacksquare$$