Lecture 20: Review of Linear Algebra

Summary:
We review essential concepts in linear algebra, focusing on vector spaces, subspaces, and linear transformations. We examine the fundamental subspaces of a matrix and prove the rank-nullity theorem. We explore orthogonality and its applications to coding theory, establishing connections between vector spaces and linear codes.

Topics Covered: basis, dimension, image, kernel, linear code, linear transformation, orthogonality, subspace, vector space

Review of linear algebra

Let $\mathcal{V}$ be a vector space over a field $\mathbb{F}$.

In $\mathcal{V}$, we have linear combinations of the form

$$av + bw$$

where $a, b \in \mathbb{F}$ and $v, w \in \mathcal{V}$.

$\mathcal{W} \subseteq \mathcal{V}$ is a subspace of $\mathcal{V}$ means it is closed under linear combinations

If we have two vector spaces $\mathcal{V}, \mathcal{V}'$ over $\mathbb{F}$, a function $T : \mathcal{V} \to \mathcal{V}'$ is called a linear transformation when it preserves linear combinations

A linear transformation has two fundamental subspaces

$$\ker(T) = \{v \in \mathcal{V} \;:\; T(v) = \vec{0}\} \subseteq \mathcal{V}$$

$$\operatorname{im}(T) = \{v' \in \mathcal{V}' \;:\; \exists v \in \mathcal{V}.\ T(v) = v'\} \subseteq \mathcal{V}'$$

Note that $\ker(T)$ and $\operatorname{im}(T)$ are subspaces, meaning they are closed under linear combinations.

A basis of a vector space is a set of vectors that are linearly independent and span the space.

Every basis has the same cardinality, and we call that $\dim \mathcal{V}$.

Rank nullity theorem:

$$\dim \mathcal{V} = \dim \ker(T) + \dim \operatorname{im}(T)$$

Exercise:

Let $\mathbb{F} = \mathbb{F}_q$ be a field with q elements.

1. Let $\mathcal{V} = \mathbb{F}_q^n$. What is $\dim \mathcal{V}$ and $|V|$?
2. Let $\mathcal{W} \subseteq \mathcal{V}$ be a subspace with $\dim \mathcal{W} = k$. What does Lagrange's theorem tell us?

Part 1:

$$|\mathcal{V}| = q^n$$

$$\dim V = n$$

Part 2:

Note that $(\mathcal{W}, +)$ is a subgroup of $(\mathcal{V}, +)$. Both groups are finite. By Lagrange's theorem, we know that $|\mathcal{W}|$ divides $|\mathcal{V}|$.

Suppose that $\mathcal{V} = \mathbb{F}^n$.

$v, w \in \mathcal{V}$ are orthogonal means $v \cdot w = \sum_{i=1}^n v_i \cdot w_i = v^T w = 0$, where

$$v = (v_1, \ldots, v_n) \in \mathbb{F}^n$$

$$w = (w_1, \ldots, w_n) \in \mathbb{F}^n$$

Let $\mathcal{W} \subseteq \mathcal{V}$ be a subspace. We denote the orthogonal subspace

$$\mathcal{W}^\perp = \{v \in \mathcal{V} \ : \ \forall w \in \mathcal{W}. \ v \cdot w = 0\}$$

Note that

$$\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^\perp$$

Which means

1. $\mathcal{V} = \mathcal{W} + \mathcal{W}^\perp$
2. $\mathcal{W} \cap \mathcal{W}^\perp = \{0\}$

Therefore, when $\dim \mathcal{W}, \dim \mathcal{W}^\perp < \infty$, we have that

$$\dim \mathcal{V} = \dim \mathcal{W} + \dim \mathcal{W}^\perp$$

Views of linear combinations:

Row vector multiplication on the left

$$[x_1 \quad x_2] \begin{bmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{bmatrix} = x_1[\alpha \, \alpha' \, \alpha''] + x_2[\beta \, \beta' \, \beta'']$$

Column vector multiplication on the right

$$\begin{bmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = y_1 \begin{bmatrix} \alpha \\ \beta \end{bmatrix} + y_2 \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} + y_3 \begin{bmatrix} \alpha'' \\ \beta'' \end{bmatrix}$$

4 subspaces of a matrix A:

$$A \in \mathbb{F}^{m \times n}$$
$$T : \mathbb{F}^m \to \mathbb{F}^n$$
$$T(y) = Ay$$

- $\ker T = \{y \in \mathbb{F}^m \ : \ Ay = 0\}$ is called the **kernel** or **right nullspace** of A
- $\operatorname{im} T$ is called the **image** or **column space** of A

$$\tilde{T} : \mathbb{F}^n \to \mathbb{F}^m$$
$$\tilde{T}(x) = xA$$

- $\ker \tilde{T}$ is called the **left nullspace** of A
- $\operatorname{im} \tilde{T}$ is called the **row space** of A

Theorem:

Fix $A \in \mathbb{F}^{n \times m}$. Then, we have

$$\text{nullspace}(A) = \text{rowspace}(A)^\perp$$

Note that

$$y \in \text{null}(A) \iff Ay = 0 \iff \text{dot productof every row of A with y is 0}$$
$$\iff \text{y is orthogonal to every row of A}$$
$$y \in \text{row}(A)^\perp$$

Reminder:

$$\dim \text{row } A = \dim \text{col } A = \text{rank } A$$

Graphs:

Each vertex represents a vector and each edge represents the difference of two vectors $e_i - e_j$.

$$S_G = \{e_i - e_j \ : \ (i,j) \in G, \ i < j\}$$
$$\mathcal{V} = \mathrm{span}_{\mathbb{R}} S_G$$

Bases for a graph-based vector space:

A basis corresponds to an MST of the graph.

An MST is a minimal subset of edges that spans the graph.

Definition:

A linear code C is a vector subspace of $\mathbb{F}_q^m$. Furthermore, if $\dim C = n$, then call it an $[m, n]$ code.

Let C be a 3-fold repitition code over $\mathbb{F}_2$ with message length 2.

$$C = \{00000, 101010, 010101, 111111\} \subseteq \mathbb{F}_2^6$$

Note that C is a subspace of $\mathbb{F}_q^m$.

$$= \mathrm{span}\{y_2, y_3\}$$

Then, we have $y_2 + y_3 = y_4$.

The Hamming distance of C is

$$d(C) = 3$$

Lemma 1:

Let C be a linear code. Then,

$$d(C) = \min\{w(y) \ : \ y \in C\}$$

- $w(y)$ denotes the weight of y

Proof:

By definition, we have

$$d(C) = \min\{d(x,y) \ : \ x, y \in C, x \neq y\}$$

Note that $d(x,y) = w(x-y)$.

Let $x, y \in C$. Then, we have

$$d(x,y) = w(x-y)$$

And, since C is a subspace, we have

$$x - y \in C$$