MA-GY 7043: Linear Algebra II

Orthogonal Projection
Construction of Unitary Basis
Adjoint Maps and Matrices
Unitary Transformations and Matrices

Deane Yang

Courant Institute of Mathematical Sciences
New York University

February 20, 2025

Outline I

Orthogonal Projection Using an Orthonormal Set (Part 1)

- Let $(u_1, \ldots, u_k)$ be an orthonormal basis of a subspace $E \subset V$
- For any $v \in E$, there exist $a^1, \ldots, a^k \in \mathbb{F}$ such that

$$v = a^1 u_1 + \cdots + a^k u_k$$

- Since, for each $1 \leq j \leq k$,

$$(v, u_j) = (a^1 u_1 + \cdots + a^k u_k, u_j) = a^j,$$

it follows that

$$v = (v, u_1)u_1 + \cdots + (v, u_k)u_k$$

Orthogonal Projection Using an Orthonormal Set (Part 2)

- Consider the map $\pi_E : V \to E$ given by

$$\pi_E(v) = (v, u_1)u_1 + \cdots + (v, u_k)u_k$$

- For any $v \in V$ and $1 \leq j \leq k$,

$$(v - \pi_E(v), u_k) = (v, u_k) - (v, u_k) = 0$$

  and therefore

$$v - \pi_E^{\perp}(v) \in E^{\perp}$$

- Therefore, if for any v,

$$\pi_E^{\perp}(v) = v - \pi_E(v),$$

  then

$$v = \pi_E(v) + \pi_E^{\perp}(v)$$

- It follows that, if E has an orthonormal basis, then

$$E \oplus E^{\perp} = V$$

Constructing an Orthonormal Basis of V (Part 1)

- Let E be a k-dimensional subspace of V, with $k \geq 1$
- Let $(v_1, \ldots, v_k)$ be a basis of E
- For each $1 \leq j \leq k$, let

$$E_j = \mathrm{span}(v_1, \ldots, v_j)$$

- We can construct an orthonormal set that spans E by induction
- Let

$$u_1 = \frac{v_1}{|v_1|},$$

- Then $\{u_1\}$ is an orthonormal basis of E_1

Constructing an Orthonormal Basis (Part 2)

- Assume that $j < k$ and that $(u_1, \ldots, u_j)$ is an orthonormal basis of $E_j \subset E$
- Let
$$v_{j+1} = \pi_{E_j}(v_{j+1}) + \pi^{\perp}_{E_j}(v_{j+1}),$$
where
$$\begin{aligned}\pi_{E_j}(v_{j+1}) &= (v_{j+1}, u_1)u_1 + \cdots + (v_{j+1}, u_j)u_j \in E_j \\ \pi^{\perp}_{E_j}(v_{j+1}) &= v_{j+1} - \pi_{E_j}(v_{j+1}) \in E_j^{\perp}\end{aligned}$$
- Since $v_{j+1} \notin E_j$ and $\pi_{E_j}(v_{j+1}) \in E$, it follows that
$$\pi^{\perp}_{E_j}(v_{j+1}) \neq 0$$
- Let
$$u_{j+1} = \frac{\pi^{\perp}_{E}(v_{j+1})}{|\pi^{\perp}_{E}(v_{j+1})|}$$
- Since $u_{j+1} \in E_j^{\perp}$, $(u_{j+1}, u_i) = 0$ for all $1 \leq i \leq j$
- Therefore, $(u_1, \ldots, u_{j+1})$ is an orthonormal basis of E_{j+1}

Gram-Schmidt Construction of Orthonormal Basis

- Let $(v_1, \ldots, v_n)$ be a basis of an inner product space V
- There exists an orthonormal basis $(u_1, \ldots, u_n)$ such that for each $1 \leq k \leq n$,

$$\mathrm{span}(u_1, \ldots, u_k) = \mathrm{span}(v_1, \ldots, v_k)$$

Unitary Set

- Let V be a complex vector space
- A set $\{e_1, \ldots, e_k\}$ is called **unitary** if

$$(e_i, e_j) = \delta_{ij}, 1 \leq i, j \leq k$$

- If $v = a^1 e_1 + \cdots + a^k e_k$, then for each $1 \leq j \leq k$,

$$\begin{aligned}(v, e_j) &= (a^1 e_1 + \cdots + a^k e_k, e_j) \\ &= a^1 (e_1, e_j) + \cdots + a^k (e_k, e_j) \\ &= a_j\end{aligned}$$

- It follows that a unitary set is linearly independent
  - If $a^1 e_1 + \cdots + a^k e_k = 0$, then for each $1 \leq j \leq k$,

$$a^j = (a^1 e_1 + \cdots + a^k e_k, e_j) = 0$$

- If $\dim V = n$, then a unitary set with n elements is a **unitary basis**

Gram-Schmidt

- **Lemma.** *Any (possibly empty) unitary set can be extended to a unitary basis*
- Suppose $S = \{e_1, \ldots, e_k\}$ is a unitary set, where $k < \dim V$
- The span of S is not all of V and therefore there is a nonzero vector $v \in V$ such that $v \notin S$
- Let $\hat{v} = v - (v, e_1)e_1 - \cdots - (v, e_k)e_k$
- $\hat{v} \neq 0$, because $v \notin$ the span of S
- $\hat{v}$ is orthogonal to S, because for each $1 \leq j \leq k$,

  $$(\hat{v}, e_j) = (v - (v, e_1)e_1 - \cdots - (v, e_k)e_k, e_j) = (v, e_j) - (v, e_j) = 0$$

- If

  $$e_{k+1} = \frac{\hat{v}}{\|\hat{v}\|},$$

  then $\|e_{k+1}\| = 1$ and $(e_{k+1}, e_j) = 0$ for each $1 \leq j \leq k$
- Therefore, $\{e_1, \ldots, e_{k+1}\}$ is a unitary set

Adjoints of Linear Maps and Matrices (Part 1)

- Let V, W be inner product spaces and $L : V \to W$ be a linear map
- The **(Hermitian) adjoint** of L is defined to be the map $L^* : W \to V$ such that for any $v \in V$ and $w \in W$,

$$(L(v), w) = (v, L^*(w))$$

- If M is an m-by-n matrix, its **(Hermitian) adjoint** is defined to be the n-by-m matrix

$$M^* = \overline{M}^T$$

Adjoints of Linear Maps and Matrices (Part 2)

- Let
$$E = \begin{bmatrix} e_1 & \dots & e_n \end{bmatrix}$$
be a unitary basis of V and
$$F = \begin{bmatrix} f_1 & \dots & f_m \end{bmatrix}$$
be a unitary basis of W
- Let $L : V \to W$ be a linear map and M be the matrix such that
$$LE = FM,$$
- Let $L^* : W^* \to V^*$ be the adjoint of L and N be the matrix such that
$$L^*F = EN$$

Adjoints of Linear Maps and Matrices (Part 3)

- For any vectors

$$v = e_1 a^1 + \cdots + e_n a^n = Ea \text{ and } w = f_1 b^1 + \cdots + f_m b^m = Fb,$$

we get

$$\begin{aligned}
(L(v), w)) &= (LEa, Fb) \\
&= (FMa, Fb) \\
&= (f_p M^p_j a^j, f_q \bar{b}^q) \\
&= (f_p, f_q) M^p_j a^j \bar{b}^q \\
&= \delta_{pq} M^p_j a^j \bar{b}^q \\
&= \sum_{j=1}^{m} \sum_{p=1}^{n} M^p_j a^j \bar{b}^p
\end{aligned}$$

Adjoints of Linear Maps and Matrices (Part 4)

- On the other hand,

$$
\begin{aligned}
(v, L^*(w)) &= (Ea, L^*(Fb)) \\
&(Ea, ENb) \\
&= (e_j a^j, e_k N^k_p b^p) \\
&= (e_j, e_k) a^j \bar{N}^k_p \bar{b}^p \\
&= \delta_{jk} a^j \bar{N}^k_p \bar{b}^p \\
&= \sum_{j=1}^{m} \sum_{p=1}^{n} \bar{N}^j_p a^j \bar{b}^p
\end{aligned}
$$

- Since $(L(v), w) = (v, L^*(w))$ for all $v \in V$ and $w \in W$, it follows that

$$\bar{N}^j_p = M^p_j, \text{ i.e., } N^j_p = \bar{M}^p_j,$$

or equivalently,

$$N = M^*$$

Adjoints of Linear Maps and Matrices (Part 5)

- If E is a unitary basis of V and F is a unitary basis of W, $L : V \to W$ is a linear map, and M is a matrix that satisfies

$$L(E) = FM,$$

then

$$L^*(F) = EM^*$$

Basic Properties of Adjoint Map

- If $L, L_1, L_2 : V \to W$ are linear maps and $c \in \mathbb{F}$, then

$$
\begin{aligned}
(L_1 + L_2)^* &= L_1^* + L_2^* \\
(cL)^* &= \bar{c}L^* \\
(L_1 \circ L_2)^* &= L_2^* \circ L_1^* \\
(L^*)^* &= L \\
(w, L(v)) &= (L^*(w), v)
\end{aligned}
$$

Fundamental Subspaces of Adjoint Map

- Let $L : V \to W$ be a map between inner produt spaces
- Then

$$\ker(L^*) = (\text{image}(L))^\perp \tag{1}$$

$$\ker(L) = (\text{image}(L^*))^\perp \tag{2}$$

$$\text{image}(L) = (\ker(L^*))^\perp \tag{3}$$

$$\text{image}(L^*) = (\ker(L))^\perp \tag{4}$$

- That
  - For any subspace S, $(S^\perp)^\perp = S$
  - For any linear map A, $(A^*)^* = A$

  imply that (2),(3),(4) follow directly from (1)

Proof that $\ker(L^*) = (\text{image}(L))^\perp$

$$
\begin{aligned}
w \in \ker(L^*) &\iff L^*(w) = 0 \\
&\iff \forall v \in V,\ (v, L^*(w)) = 0 \\
&\iff \forall v \in V,\ (L(v), w) = 0 \\
&\iff w \in (\text{image}(L))^\perp
\end{aligned}
$$

Geometric Description of a Linear Map and its Adjoint

- Recall that if E is a subspace of V, then
$$V = E \oplus E^\perp$$
- Therefore,
$$V = (\ker(L)) \oplus (\ker(L))^\perp$$
- It is easy to show that the restriction of L to $(\ker(L))^\perp$,
$$L : (\ker(L))^\perp \to \text{image}(L)$$
is bijective
- Equivalently, by (4),
$$L : \text{image}(L^*) \to \text{image}(L)$$
is bijective
- Therefore,
$$\text{rank}(L) = \dim(\text{image}(L)) = \dim(\text{image}(L^*)) = \text{rank}(L^*)$$

Isometries

- A map (not assumed to be linear) $L : V \to W$, where V and W are normed vector spaces, is an **isometry** if for any $v \in V$,

$$|L(v)| = |v|$$

- **Theorem:** If V and W are inner product spaces and $L : V \to W$ is an isometry, then L is linear and satisfies for any $v_1, v_2 \in V$,

$$(L(v_1), L(v_2)) = (v_1, v_2)$$

- **Lemma:** $L : V \to W$ is an isometry if and only if $L^* \circ L = I_V$, i.e., L^* is a left inverse of L
- In particular, if $L(v) = 0$, then

$$v = L^*(L(v)) = 0$$

  and therefore, $\ker(L) = \{0\}$
- It follows that if $L : V \to W$ is an isometry, then

$$\dim(V) \leq \dim(W)$$

Basic Properties of Isometries

- If $L : V \to W$ is an isometry and $(v_1, \ldots, v_n)$ is an unitary basis of V, then $(L(v_1), \ldots, L(v_n))$ is an unitary set in W
- If $L_1 : V \to W$ and $L_2 : W \to X$ are unitary, then so is $L_2 \circ L_1 : V \to X$

Unitary Transformation

- If $W = V$, then an isometry $L : V \to V$ is called a **unitary transformation**
- If V is an inner product space, a linear transformation $L : V \to V$ is **unitary**, if for any $v, w \in V$, if any of the following equivalent statements hold:

$$(L(v), L(w)) = (v, w)$$
$$(L^* L(v), w) = (v, w)$$
$$L^* \circ L = I$$
$$L \text{ is invertible and } L^{-1} = L^*$$

Unitary Matrices

- Let $L : V \to V$ be a unitary map
- If $(u_1, \ldots, u_n)$ is a unitary basis of V and $L(u_k) = M^j_k u_j$, then

$$\begin{aligned}\delta_{jk} &= (u_j, u_k) \\ &= (L(u_j), L(u_k)) \\ &= (u_j, (L^* \circ L)(u_k)) \\ &= (u_j, (M^* M)^i_k u_i) \\ &= (M^* M)^j_k\end{aligned}$$

- $$M^* M = I$$
- A matrix M is **unitary** if $M^* M = M M^* = I$

Examples of Unitary Matrices

- An n-by-n matrix is unitary if and only if its columns form a unitary basis of $\mathbb{F}^n$
- A real 2-by-2 matrix is a unitary matrix with positive determinant if and only if it is of the form

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

- For any $\theta^1, \theta^2 \in \mathbb{R}$

$$\begin{bmatrix} e^{i\theta^1} & 0 \\ 0 & e^{i\theta^2} \end{bmatrix}$$

More Properties of Unitary Matrices

- Let U be a unitary matrix
- $\det(U^*) = \overline{\det(U)}$
  - Because $\det(A^T) = \det(A)$ and $\det(\overline{A}) = \overline{\det(A)}$
- If λ is an eigenvalue of U, then $|\lambda| = 1$
  - Because if λ is an eigenvalue of U with eigenvector v, then

    $$|v| = |Uv| = |\lambda v| = |\lambda||v|,$$

    which implies $|\lambda| = 1$

Properties of unitary maps and matrices

- If L_1, L_2 are unitary maps, then so is $L_1 \circ L_2$
  - If M_1, M_2 are unitary matrices, then so is $M_1 M_2$
- If L is unitary, then L is invertible and $L^{-1} = L^*$ is unitary
  - If M is unitary, then M is invertible and $M^{-1} = M^*$ is unitary
- The identity map is unitary
  - The identity matrix is unitary

Unitary Group

- Define the unitary group $U(V)$ of a Hermitian vector space V to be the set of all unitary transformations
- Denote
$$U(n) = U(\mathbb{C}^n)$$
using the standard Hermitian inner product on $\mathbb{C}^n$
- Both satisfy the properties of an abstract group G
  - Any ordered pair $(g_1, g_2) \in G \times G$ uniquely determine a third, denoted $g_1 g_2 \in G$
  - (Associativity) $(g_1 g_2) g_3 = g_1 (g_2 g_3)$
  - (Identity element) There exists an element $e \in G$ such that $ge = eg = g$ for any $g \in G$
  - (Inverse of an element) For each $g \in G$, there exists an element $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$
- $U(n)$ is an example of a matrix group
- Both $U(V)$ and $U(n)$ are examples of Lie groups