Linear Algebra II Note

陳信睿

January, 2023

Abstract

這篇筆記主要是因爲在預習線性代數二的時候，常常發現很多重要的定理都記不太起來，並且老師在下學期沒有選定指定的參考書，所以我就寫了這份筆記。主要是參考謝銘倫老師的影片 [3]，以及著名的線性代數教科書 [2] 所寫。

內容目前涵蓋了商空間、對偶空間以及內積空間的大部分內容，甚至比 "Linear Algebra"[2] 中還要多東西，像是 Hilbert space。不過我盡量把證明寫的精簡一點，同時我也省去了所有的範例。

I wrote this note because I often found that I could not remember many important theorems when I was studying Linear Algebra II, and my teacher did not choose a reference book for the next semester. The main reference is Professor Ming-Lun Hsieh's video [3], and the famous linear algebra textbook [2].

The content now covers most of the quotient space, dual space, and inner product space, even more than in "Linear Algebra"[2], like Hilbert space. I have tried to keep the proof as concise as possible, and I have also omitted all the examples.

Contents

1 Quotient and dual spaces

1.1 Quotient space

Definition 1 (Quotient space)**.** Let V be a vector space and let W be its subspace. Define an equivalence relation $\sim$ on V such that

$$v_1 \sim v_2 \text{ if } v_1 - v_2 \in W.$$

It is easy to verify that $\sim$ is indeed an equivalence relation on V. For each $v_0 \in V$, define $[v_0] = \{v \in V : v \sim v_0\}$ the equivalence class of v_0. Then, $\{[v] : v \in V\}$ is called the quotient space V/W.

Remark. The quotient space V/W is equipped with a natural linear structure, namely,

$$\begin{cases} [v_1] + [v_2] = [v_1 + v_2], & \text{for all } v_1, v_2 \in V \\ c[v_1] = [cv_1], & \text{for all } v_1 \in V \text{ and } c \in F \end{cases}$$

Although it is crucial that we shall check these natural addition and scalar multiplication are "well-defined", we omit here.

Definition 2 (Quotient maps)**.** There is a natural surjective map

$$\begin{aligned} \pi : V &\to V/W \\ v &\mapsto [v] \end{aligned}$$

which is called the quotient map. Moreover, it is a linear transformation.

Remark.

$$\begin{aligned} \ker \pi &= \{v \in V : \pi(v) = [0]\} \\ &= \{v \in V : [v] = [0]\} \\ &= \{v \in V : v - 0 \in W\} \\ &= W. \end{aligned}$$

Corollary. It follows from the dimension formula that $\dim_F V/W = \dim_F V - \dim_F W$ whenever V is finite dimensional.

Here we give an alternative proof without using the dimensional formula. Since V has finite dimension, let $\mathcal{B} = \{w_1, w_2, \dots, w_s\}$ be a basis of W and extend $\mathcal{B}$ to $\mathcal{A} = \{w_1, w_2, \dots, w_r\}$ a basis of V. We claim that $\{[w_{s+1}], \dots, [w_s]\}$ is a basis of V/W. To see this, we shall show that:

1. The set $\{[w_{s+1}], \dots, [w_r]\}$ generates V/W.
Suppose $[v] \in V/W$. Let $v = \sum_{i=1}^{r} \alpha_i w_i$, then

$$[v] = \left[\sum_{i=s+1}^{r} \alpha_i w_i\right] = \sum_{i=s+1}^{r} \alpha_i [w_i] \quad .$$

2. $\{[w_{s+1}], \dots, [w_r]\}$ is a linear independent set over F.
Suppose $\sum_{i=s+1}^{r} \alpha_i \cdot [w_i] = [0]$, for some $\alpha_i \in F$. Then,

$$\left[\sum_{i=s+1}^{r} \alpha_i w_i\right] = [0]$$

$$\iff \sum_{i=s+1}^{r} \alpha_i w_i \in W$$

$$\iff \sum_{i=s+1}^{r} \alpha_i w_i = \sum_{j=1}^{s} \beta_j w_j, \text{ for some } \beta_j \in F.$$

We conclude that α_i are all zeros, since $\mathcal{A}$ is a basis of V.

Discussions above show that $\dim_F V/W = r - s = \dim_F V - \dim_F W$. Now, we shall study some properties about the quotient space V/W. The next theorem characterize the quotient space V/W by the following universal property.

Theorem 3. *Let T be a linear transformation from V to U, such that* $\ker T$ *contains W, namely $W \subset \ker T$. Then, T factors through π uniquely. That is, there exists a unique linear transformation $S : V/W \to U$ such that*

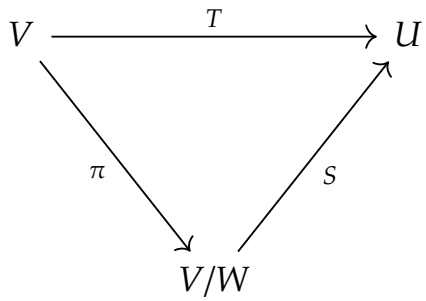
$$T = S \circ \pi.$$

Proof. Define $S : V/W \to U$ by

$$S([v]) = T(v).$$

We first show that S is a well-defined map, namely, if $[v] = [v']$, then $T(v) = T(v')$. Note that $[v] = [v'] \implies v - v' \in W \subset \ker T$, we conclude $T(v) = T(v')$. By definition, S is a linear transformation and $S \circ \pi = T$. The uniqueness of such S follows from the surjectivity of π. □

Theorem 3 implies that the following diagram commutes.



Remark. The quotient space V/W with the quotient map π is the unique vector space satisfying the theorem. That is, if we are given $\pi' : V \to V'$ satisfying the property: for every linear transformation $T : V \to U$ with $W \subset \ker T$, there exists a unique $S' : V' \to U$ such that $S' \circ \pi' = T$. Then, $V' \simeq V/W$ uniquely.

Proof. From the assumptions, we have

$$\begin{cases} \exists!\ S : V/W \to V', \text{ such that } \pi' = S \circ \pi \\ \exists!\ S' : V' \to V/W, \text{ such that } \pi = S' \circ \pi' \end{cases}.$$

This shows $S \circ S' = \mathrm{Id}_{V'}$; $S' \circ S = \mathrm{Id}_{V/W}$ (using Theorem 3 again.) We conclude $V' \simeq V/W$ uniquely. □

Corollary. Let $T : V \to W$ be a linear transformation. Then,

$$V/\ker T \simeq \mathrm{Im}T.$$

Hence, $\dim_F V/\ker T = \dim_F \mathrm{Im}T$.

Proof. From Theorem 3, we have: there exists a unique $S : V/\ker T \to W$, such that $T = S \circ \pi$. It follows from the surjectivity of π that $\mathrm{Im}S = \mathrm{Im}T$. We claim that S is injective. Note that

$$\begin{aligned}\ker S &= \{[v] \in V/\ker T : S([v]) = 0\} \\ &= \{[v] \in V/\ker T : T(v) = 0\} \\ &= \{[v] \in V/\ker T : v \in \ker T\} \\ &= \{[0]\}.\end{aligned}$$

Thus, S is a bijection. This completes the proof. □

Now, let $T : V \to V$ be a linear transformation and let $W \subset V$ be a T-invariant subspace. Then, T induce a linear transformation $\tilde{T}$ on V/W define by:

$$\begin{aligned}\tilde{T} : V/W &\to V/W \\ [v] &\mapsto [T(v)]\end{aligned}.$$

This is a well-defined map since

$$\begin{aligned}[v] = [v'] &\implies v - v' \in W \\ &\implies T(v) - T(v') = T(v - v') \in W \\ &\implies [T(v)] = [T(v')].\end{aligned}$$

Now, let $\mathcal{B} = \{v_1, v_2, \dots, v_s\}$ be a basis of W, and extend it to $\mathcal{A} = \mathcal{B} \sqcup \mathcal{B}'$, a basis of V. We have shown that $[\mathcal{B}'] = \{[v] : v \in \mathcal{B}'\}$ is a basis of V/W. Then, we have

$$[T]_{\mathcal{A}} = \left(\begin{array}{c|c} [T|_W]_{\mathcal{B}} & * \\ \hline 0 & \left[\tilde{T}\right]_{[\mathcal{B}']} \end{array}\right).$$

We thus have

$$\begin{cases} \mathrm{ch}_T(x) = \mathrm{ch}_{T|_W}(x) \cdot \mathrm{ch}_{\tilde{T}}(x) \\ \mathrm{m}_T(x) \text{ is divisible by } \mathrm{m}_{T|_W}(x) \end{cases}.$$

Corollary. If T is diagonalizable, then so is $\tilde{T}$.

The corollary follows from the fact that $\mathrm{m}_T(x)$ is divisible by $\mathrm{m}_{\tilde{T}}(x)$. We next shall discuss the concept of dual spaces.

1.2 Dual space

Definition 4 (Dual space)**.** Let V be a vector space over F. It is well-known that $L(V,F)$ is a vector space over F. It is called the dual space of V, and its elements are called linear functionals of V. We often write $V^\vee$ to denote the dual space of V.

Recall that:

> Given two vector spaces V, W over F. Then we have $L(V,W)$ is a vector space over F and
>
> $$\dim_F L(V,W) = \dim_F V \cdot \dim_F W.$$

We conclude that $\dim_F V^\vee = \dim_F V$ if $\dim_F V < \infty$. Here we give an alternative proof.

Theorem 5. *Suppose V is a finite dimensional vector space over F. Then,* $\dim_F V^\vee = \dim_F V$.

Proof. Let $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ be a basis of V. Let us consider the following linear functionals:

$$v_i^\vee : V \to F$$

$$\sum_{i=1}^n \alpha_i \cdot v_i \mapsto \alpha_i$$

We claim that $\mathcal{B}^\vee = \left\{v_1^\vee, v_2^\vee, \dots, v_n^\vee\right\}$ is a basis of $V^\vee$. We first show that $\mathcal{B}^\vee$ is linear independent. Suppose there exist $\beta_i \in F$ such that

$$\sum_{i=1}^n \beta_i v_i^\vee = 0,$$

then

$$\sum_{i=1}^n \beta_i v_i^\vee \left(v_j\right) = 0.$$

This shows

$$\beta_i = 0, \text{ for all } i = 1, 2, \dots, n.$$

Next we show that $\mathcal{B}^\vee$ generate $V^\vee$. Given $\ell \in V^\vee$. Then, from the linearity of ℓ, we have

$$\ell = \sum_{i=1}^n \ell(v_i) \cdot v_i^\vee.$$

We conclude that $\mathcal{B}^\vee$ is a basis of $V^\vee$. □

Remark. The basis $\mathcal{B}^\vee$ is called the dual basis of $\mathcal{B}$.

Given a linear transformation $T : V \to W$, it induces a linear transformation $T^\vee : W^\vee \to V^\vee$ between dual spaces defined by:

$$T^\vee(\ell)(v) := \ell(T(v)), \text{ for } \ell \in W^\vee \text{ and } v \in V.$$

It is easy to verify that $T^\vee$ is a linear transformation.

Theorem 6. *Let V, W be two finite dimensional vector spaces over F. Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ and $\mathcal{B} = \{w_1, w_2, \dots, w_m\}$ be bases of V and W, respectively. Given $T : V \to W$. Then,*

$$[T]^{\mathsf{t}}_{\mathcal{A},\mathcal{B}} = \left[T^\vee\right]_{\mathcal{B}^\vee,\mathcal{A}^\vee}.$$

Proof. Let $A := [T]_{\mathcal{A},\mathcal{B}} = (a_{ij})_{n\times n}$ and $B := \left[T^\vee\right]_{\mathcal{B}^\vee,\mathcal{A}^\vee} = (b_{ij})_{n\times n}$. From the definition, we have

$$\begin{aligned} T(v_j) &= \sum_{i=1}^{m} a_{ij} w_i \\ T^\vee(w_i^\vee) &= \sum_{j=1}^{n} b_{ji} v_j^\vee \end{aligned}.$$

Then,

$$b_{ji} = T^\vee(w_i^\vee)(v_j) = w_i^\vee(T(v_j)) = w_i^\vee\left(\sum_{i=1}^{m} a_{ij} w_i\right) = a_{ij}.$$

This proves the theorem. □

Theorem 7. *Let V be a vector space and let $W \subset V$ be a subspace. Then,*

$$(V/W)^\vee \simeq \left\{\ell \in V^\vee : W \subset \ker \ell\right\}.$$

Proof. We have known that there is a natural map $\pi : V \twoheadrightarrow V/W$. We claim that $\pi^\vee$ is the isomorphism that bijects $(V/W)^\vee$ and $\left\{\ell \in V^\vee : W \subset \ker \ell\right\}$. We first show that $\pi^\vee$ is injective. Suppose $\pi^\vee(\ell) = 0$, for some $\ell \in (V/W)^\vee$. Then,

$$\begin{aligned} & l(\pi(v)) = 0, \text{ for all } v \in V \\ \implies & \ell([v]) = 0, \text{ for all } v \in V. \end{aligned}$$

This shows the injectivity of $\pi^\vee$. Hence, $(V/W)^\vee \simeq \mathrm{Im}\pi^\vee$. It suffices to show that $\mathrm{Im}\pi^\vee = \left\{\ell \in V^\vee : W \subset \ker \ell\right\}$.

1. $\mathrm{Im}\pi^\vee \subset \left\{\ell \in V^\vee : W \subset \ker \ell\right\}$.
   For each $S \in (V/W)^\vee$ and $w \in W$, we have
   $$\pi^\vee(S)(w) = S(\pi(w)) = S([w]) = S([0]) = 0.$$
2. $\left\{\ell \in V^\vee : W \subset \ker \ell\right\} \subset \mathrm{Im}\pi^\vee$.
   Let $\ell \in V^\vee$ such that $W \subset \ker \ell$. Theorem 3 asserts that there exists a unique $S : V/W \to F$ such that $\ell = S \circ \pi$. This implies $\pi^\vee(S) = \ell$.

Discussions above complete the proof. □

Corollary. Let $A \in M_{m\times n}(F)$. Then, $\mathrm{rank}A = \mathrm{rank}A^{\mathsf{t}}$.

Proof. Let $V = F^n$, $W = F^m$ and let $T : V \to W$ defined by

$$T(v) = A \cdot v.$$

Then it is equivalent to prove

$$\dim \mathrm{Im}T = \dim (\mathrm{Im}T^\vee).$$

By Theorem 7,

$$(W/\mathrm{Im}T)^\vee \simeq \left\{\ell \in W^\vee : \mathrm{Im}T \subset \ker \ell\right\} = \left\{\ell \in W^\vee : T^\vee(\ell) = 0\right\} = \ker(T^\vee). \tag{1}$$

Thus,

$$\dim W - \dim \mathrm{Im}T = \dim W/\mathrm{Im}T = \dim (W/\mathrm{Im}T)^\vee = \dim W^\vee - \dim \mathrm{Im}(T^\vee).$$

This completes the proof. □

Theorem 8. *Let V and W are two finite vector spaces, and let $T : V \to W$ be a linear transformation. Then,*

1. *T is surjective if and only if $T^\vee$ is injective.*
2. *T is injective if and only if $T^\vee$ is surjective.*

Proof. In the proof of the previous corollary, we have shown in equation 1 that

$$(W/\mathrm{Im}T)^\vee \simeq \ker(T^\vee),$$

this proves the first assertion. Similarly, we have

$$(V/\ker T)^\vee \simeq \left\{\ell \in V^\vee : \ker T \subset \ker \ell\right\}. \tag{2}$$

We claim the set on the right hand side is $\mathrm{Im}(T^\vee)$.

1. $\left\{\ell \in V^\vee : \ker T \subset \ker \ell\right\} \subset \mathrm{Im}(T^\vee)$.
   Let $\ell \in V^\vee$ such that $\ker T \subset \ker \ell$. It is well-known that there exists a subspace $X \subset W$ such that $W = \mathrm{Im}T \oplus X$. Consider a transformation $s : W \to F$ defined by:

   $$s(w) = \ell(v),$$

   where $w = T(v) + x$, for some $v \in V$ and $x \in X$. This is a well-defined map, since $\ker T \subset \ker \ell$. Note that s is a linear transformation and $\ell = s \circ T = T^\vee(s)$. This implies $\left\{\ell \in V^\vee : \ker T \subset \ker \ell\right\} \subset \mathrm{Im}(T^\vee)$.

2. $\mathrm{Im}(T^\vee) \subset \left\{\ell \in V^\vee : \ker T \subset \ker \ell\right\}$.
   Let $\ell \in \mathrm{Im}(T^\vee)$. Then, there exists $s \in W^\vee$ such that $\ell = T^\vee(s) = s \circ T$, thus $\ker T \subset \ker \ell$.

Discussions above with equation 2 show that

$$(V/\ker T)^\vee \simeq \mathrm{Im}(T^\vee),$$

which is equivalent to the second assertion. □

Remark. In the class, the teacher proved with another approach, which use the following property:

Let V be a finite dimensional vector space, and let $V^{\vee\vee}$ be the dual space of $V^{\vee}$, then there is a natural identification, that is, there is an isomorphism $\phi : V \to V^{\vee\vee}$ defined by

$$\phi : x \mapsto \left(\hat{x} : f \mapsto f(x)\right), \quad f \in V^{\vee}.$$

Next, we show that why we shall study dual spaces by the following theorem.

Theorem 9. *Let V be a finite dimensional vector space over F. Let $\ell_1, \ell_2, \dots, \ell_s \in V^{\vee}$ be linearly independent. Suppose $b_1, b_2, \dots, b_s \in F$ and put*

$$\Xi = \left\{v \in V : \ell_i(v) = b_i, \text{ for all } 1 \le i \le s\right\}.$$

Then, $\Xi \neq \varnothing$.

Proof. Consider the linear transformation $T : V \to F^s$ defined by:

$$T : v \mapsto (\ell_1(v), \ell_2(v), \dots, \ell_s(v)).$$

Then, $\dim(\ker T) = \dim V - s$. Here we omit the details of the proof. □

2 Inner product space

Definition 10 (Inner product)**.** Let V be a vector space over F, where $F = \mathbb{R}$ or $\mathbb{C}$. A function $\langle\cdot,\cdot\rangle : V \times V \to F$ is called an inner product if the following conditions are satisfied:

1. $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$, for all $x, y, z \in V$.
2. $\langle cx, y\rangle = c \cdot \langle x, y\rangle$, for all $x, y \in V$ and $c \in F$.
3. $\langle x, y\rangle = \overline{\langle y, x\rangle}$, for all $x, y \in V$.
4. $\langle x, x\rangle \ge 0$, for all $x \in V$ and $\langle x, x\rangle = 0$ if and only if $x = 0$.

We write $(V, \langle\cdot,\cdot\rangle)$ for a vector space V together with an inner product structure $\langle\cdot,\cdot\rangle$. In the following text, F still stands for $\mathbb{R}$ or $\mathbb{C}$ unless otherwise stated.

We could also define the concept of norm (or length) of a vector $v \in V$.

Definition 11 (Norm)**.** For each $v \in V$, define the norm of v as $\|v\| = \langle v, v\rangle^{1/2}$.

Theorem 12 (Riesz representation Theorem on a finite dimensional space)**.** *Let $(V, \langle\cdot,\cdot\rangle)$ be an inner product space. Then,*

$$\begin{aligned} \Phi : V &\to V^{\vee} \\ v &\mapsto \Phi(v)(x) = \langle x, v\rangle \end{aligned}$$

is an isomorphism.

Proof. We first prove that Φ is injective. Note that

$$\ker \Phi = \{v \in V : \langle x, v\rangle = 0, \text{ for all } x \in V\} = \{0\}.$$

Since V is finite dimensional, we have $\dim_F V = \dim_F V^{\vee}$, thus Φ is an isomorphism. □

In other words, inner product $\langle \cdot, \cdot \rangle$ identifies V with its dual space $V^\vee$ when V is finite dimensional. We now start study how to represent an inner product structure with a matrix. Suppose V is a finite dimensional vector space, and let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be a basis of V. For any $x, y \in V$, there exist α_i, β_i such that

$$x = \sum_{i=1}^{n} \alpha_i \cdot v_i \,; \quad y = \sum_{j=1}^{n} \beta_j \cdot v_j.$$

Then,

$$\langle x, y \rangle = \left\langle \sum_{i=1}^{n} \alpha_i \cdot v_i, \sum_{j=1}^{n} \beta_j \cdot v_j \right\rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \overline{\beta_j} \left\langle v_i, v_j \right\rangle.$$

Hence, if we let

$$\Omega = \left(\left\langle v_i, v_j \right\rangle \right) \in M_n(F),$$

we have

$$\langle x, y \rangle = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \cdot \Omega \cdot \begin{pmatrix} \overline{\beta_1} \\ \overline{\beta_2} \\ \vdots \\ \overline{\beta_n} \end{pmatrix}.$$

The matrix Ω is called the matrix of $\langle \ , \ \rangle$ associated with $\mathcal{A}$.

Theorem 13 (change of basis)**.** *Let $\mathcal{B} = \{w_1, \dots, w_n\}$ be another basis of V. Assume that*

$$w_j = \sum_{i=1}^{n} a_{ij} v_i, \text{ for all } 1 \le j \le n.$$

Then,

$$\Omega' = A^{\mathrm{t}} \cdot \Omega \cdot \overline{A},$$

where Ω' is the matrix of $\langle \ , \ \rangle$ associated with $\mathcal{B}$ and $A = \left(a_{ij} \right)$.

Proof. Note that

$$\begin{aligned} \left\langle w_i, w_j \right\rangle &= \left\langle \sum_{k=1}^{n} a_{ki} v_k, \sum_{l=1}^{n} a_{lj} v_l \right\rangle \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ki} \langle v_k, v_l \rangle \overline{a_{lj}} \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} {a_{ik}}^{\mathrm{t}} \langle v_k, v_l \rangle \overline{a_{lj}}, \end{aligned}$$

This proves the theorem. □

Next, we shall ask whether we can define an inner product structure on V if we are given a matrix $\Omega \in M_n(F)$ and a basis $\mathcal{A}$ of V. The answer is no. In fact, the matrix can define an

inner product structure on finite dimensional V if and only if it is positive definite. The next theorem gives the sufficient condition for a matrix being able to define an inner product.

Theorem 14. *If $\Omega = B \cdot B^*$ for some $B \in M_n(F)$ with $\det B \neq 0$, then $\langle\ ,\ \rangle_{\Omega,\mathcal{A}}$ is an inner product for any choice of $\mathcal{A}$.*

Proof. Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be an arbitrary basis of V. It suffices to show the inner product defined by Ω satisfies the fourth axiom of Definition 10. If $x \in V$, then

$$x = \sum_{i=1}^{n} \alpha_i \cdot v_i, \text{ for some } \alpha_i \in F.$$

We have

$$\begin{aligned}
\langle x, x\rangle_{\Omega,\mathcal{A}} &:= \begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix} \cdot \Omega \cdot \begin{pmatrix}\overline{\alpha_1}\\ \overline{\alpha_2}\\ \vdots\\ \overline{\alpha_n}\end{pmatrix} \\
&= \begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix} \cdot B \cdot B^* \cdot \begin{pmatrix}\overline{\alpha_1}\\ \overline{\alpha_2}\\ \vdots\\ \overline{\alpha_n}\end{pmatrix} \\
&= (yB) \cdot (yB)^*,
\end{aligned}$$

where $y = \begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix}$ is a row vector. Write $yB = \begin{pmatrix}\beta_1 & \beta_2 & \dots & \beta_n\end{pmatrix}$. We get

$$\langle x, x\rangle_{\Omega,\mathcal{A}} = \begin{pmatrix}\beta_1 & \beta_2 & \dots & \beta_n\end{pmatrix} \cdot \begin{pmatrix}\overline{\beta_1}\\ \overline{\beta_2}\\ \vdots\\ \overline{\beta_n}\end{pmatrix} = \sum_{i=1}^{n} |\beta_i|^2 \geq 0,$$

and $\langle x, x\rangle_{\Omega,\mathcal{A}} = 0$ if and only if $y = 0$. From the assumption that $\det B \neq 0$, it follows $x = 0$ if $\langle x, x\rangle = 0$. □

Definition 15 (Hermitian and positive definite matrix)**.** Let $\Omega \in M_n(F)$. Then,

1. Ω is said to be Hermitian if $\Omega^* = \Omega$.
2. Ω is said to be positive definite if Ω is Hermitian and
$$x \cdot \Omega \cdot x^* > 0, \text{ for all row vector } x \in F^n \backslash \{0\}.$$

Remark. Let $\Omega \in M_n(F)$. Define a function $\langle \cdot, \cdot \rangle$ of two variables on the vector space $V = F^n$ by

$$\langle x, y\rangle = x \cdot \Omega \cdot y^*, \text{ where } x \text{ and } y \text{ are row vectors.}$$

Then, $\langle\ ,\ \rangle$ is an inner product on V if and only if Ω is positive definite.

2.1 Orthogonal projection

Definition 16 (Perpendicular)**.** Let $(V, \langle\ ,\ \rangle)$ be an inner product space. Then, we say a vector v is perpendicular to w if

$$\langle v, w \rangle = 0.$$

We often write $v \perp w$ to indicate two vectors are perpendicular to each other.

Note that the Pythagorean theorem holds, that is, $\|v + w\|^2 = \|v\|^2 + \|w\|^2$ if $\langle v, w \rangle = 0$. Now, we can define orthogonal projection of x to y.

Definition 17 (Orthogonal projection)**.** Given two vectors $x, y \in (V, \langle\ ,\ \rangle)$ $(y \neq 0)$. $\mathrm{Proj}_y(x)$ is the vector satisfying the following two conditions:

1. $\mathrm{Proj}_y(x)$ is parallel to y.
2. $x - \mathrm{Proj}_y(x) \perp y$.

From this definition, we can assume that $\mathrm{Proj}_y(x) = \alpha \cdot y$, for some $\alpha \in F$. Since $x - \mathrm{Proj}_y(x) \perp y$, we have

$$\langle x - \alpha \cdot y, y \rangle = 0 \iff \alpha = \frac{\langle x, y \rangle}{\langle y, y \rangle}.$$

We conclude that

$$\mathrm{Proj}_y(x) = \frac{\langle x, y \rangle}{\|y\|^2} \cdot y.$$

Lemma 1. Let $x, y \in (V, \langle\ ,\ \rangle)$ $(y \neq 0)$. Then,

$$\left\| \mathrm{Proj}_y(x) \right\| \leq \|x\|.$$

Moreover, the equality holds if and only if x is parallel to y.

Proof. It follows from the Pythagorean theorem. □

Corollary. $|\langle x, y \rangle| \leq \|x\| \|y\|$, holds for all $x, y \in V$.

It immediate follows from Lemma 1. This inequality is known as "Cauchy's inequality".

Corollary. $\|x + y\| \leq \|x\| + \|y\|$, holds for all $x, y \in V$.

Proof. It is equivalent to prove $\|x + y\|^2 \leq (\|x\| + \|y\|)^2$.

$$\begin{aligned}
& \|x + y\|^2 \leq (\|x\| + \|y\|)^2 \\
\iff \quad & \langle x + y, x + y \rangle \leq \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 \\
\iff \quad & \|x\|^2 + \langle x, y \rangle + \langle y, x \rangle + \|y\|^2 \leq \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 \\
\iff \quad & \Re\langle x, y \rangle \leq \|x\| \cdot \|y\|.
\end{aligned}$$

Note that $\Re\langle x, y \rangle \leq |\langle x, y \rangle| \leq \|x\| \cdot \|y\|$. This proves the corollary. □

In general, if we were given a subspace $W \subset V$, we can discuss about $\text{Proj}_W(x)$, the orthogonal projection of x to W.

Definition 18 (Generalization of orthogonal projection)**.** Let W be a subspace of V and let x be a vector in V. Then, $\text{Proj}_W(x)$ is the vector satisfying the following two conditions:

1. $\text{Proj}_W(x) \in W$.
2. $x - \text{Proj}_W(x) \perp W$. That is, $x - \text{Proj}_W(x)$ is perpendicular to any vectors in W.

The existence of $\text{Proj}_W(x)$ in a finite dimensional vector space V follows from the following theorem.

Theorem 19. *Let V be a finite dimensional inner product space and let W be a subspace of V. Define $W^\perp$ as*

$$W^\perp := \left\{v \in V : \langle v, w\rangle = 0, \textit{ for all } w \in W\right\}.$$

Then, $W^\perp$ is a subspace. Moreover, $V = W \oplus W^\perp$.

Proof. It is easy to see that $W^\perp$ is a subspace of V. Recall Theorem 12, we have an isomorphism:

$$\begin{aligned} V &\simeq V^\vee \\ v &\mapsto \ell_v(x) = \langle x, v\rangle . \end{aligned}$$

Note that the image of $W^\perp$ under this map is

$$\left\{\ell \in V^\vee : W \subset \ker \ell\right\}.$$

By Theorem 7, we have

$$W^\perp \simeq (V/W)^\vee .$$

Thus,

$$\begin{aligned} \dim_F V &= \dim_F W + (\dim_F V - \dim_F W) \\ &= \dim_F W + \dim_F V/W \\ &= \dim_F W + \dim_F W^\perp. \end{aligned}$$

We claim that $W \cap W^\perp = \{0\}$. Suppose $x \in W \cap W^\perp$, then $\langle x, x\rangle = 0$. This shows that x must be 0. We conclude that

$$V = W \oplus W^\perp.$$

□

If we are given a subspace $W \subset V$ and a vector x, then according to Theorem 19, there exist unique vectors $w_x \in W$, $w_x' \in W^\perp$ such that

$$x = w_x + w_x'.$$

We define $\text{Proj}_w(x) := w_x$. We now discuss a new idea of (external) direct sum of vector spaces.

Definition 20 (Direct sum)**.** Let V_1, V_2 be two vector spaces. Define

$$V_1 \oplus V_2 := \{(v_1, v_2) \in V_1 \times V_2\}.$$

This space has a natural linear structure:

$$(v_1, v_2) + (v_1', v_2') := (v_1 + v_1', v_2 + v_2')$$
$$c(v_1, v_2) := (c \cdot v_1, c \cdot v_2)$$

We shall say $V_1 \oplus V_2$ is the external direct sum of V_1 and V_2.

We can check that:

If W_1, W_2 are two subspaces of V, such that $W_1 \cap W_2 = \{0\}$. Then,

$$W_1 \oplus_{\text{in}} W_2 \simeq W_1 \oplus_{\text{out}} W_2,$$

where $\oplus_{\text{in}}$ is the original (internal) direct sum.

2.2 Orthonormal basis and Gram-Schimdt process

Definition 21 (Orthonormal basis)**.** A set of vectors $\{v_\alpha : \alpha \in \Lambda\}$ is an orthonormal set if $\left\langle v_\alpha, v_\beta \right\rangle = 0$ whenever $\alpha \neq \beta$, and $\left\| v_\alpha \right\| = 1$ for all $\alpha \in \Lambda$. An orthonormal basis is an orthonormal set which is a basis.

Lemma 2. If $\{v_1, v_2, \dots, v_r\}$ is an orthonormal set, then it is linearly independent.

Proof. Suppose there exist $\alpha_i \in F$ such that

$$\sum_{i=1}^{r} \alpha_i \cdot v_i = 0.$$

Then,

$$0 = \langle 0, v_i \rangle = \left\langle \sum_{i=1}^{r} \alpha_i \cdot v_i, v_i \right\rangle = \alpha_i.$$

This completes the proof. □

Remark.

1. If $\dim_F V < \infty$, then any orthonormal set of cardinality equal to n is an orthonormal basis.

2. Let $\mathcal{A}$ be an orthonormal basis. Then, $\Omega = I_n$, where Ω is the matrix of $\langle\ ,\ \rangle$ associated with $\mathcal{A}$.

The existence of orthonormal bases in a finite dimensional inner product space follows from the next theorem. The technique to find such a basis is known as Gram-Schmidt process.

Theorem 22 (Gram-Schmidt process)**.** *Suppose* $\{v_1, v_2, \dots, v_r\}$ *is linearly independent. Then, there exists an orthonormal set* $\{w_1, w_2, \dots, w_r\}$ *such that*

$$\operatorname{span}_F\{w_1, w_2, \dots, w_r\} = \operatorname{span}_F\{v_1, v_2, \dots, v_r\}.$$

Proof. Define u_i and w_i recursively as:

$$\begin{aligned}
u_1 &= v_1 & w_1 &= \frac{u_1}{\|u_1\|} \\
u_2 &= v_2 - \langle v_2, w_1\rangle \cdot w_1 & w_2 &= \frac{u_2}{\|u_2\|} \\
u_3 &= v_3 - \langle v_3, w_2\rangle \cdot w_2 - \langle v_3, w_1\rangle \cdot w_1 & w_3 &= \frac{u_3}{\|u_3\|} \\
&\vdots & &\vdots \\
u_k &= v_k - \sum_{i=1}^{k} \langle v_k, w_i\rangle \cdot w_i & w_k &= \frac{u_k}{\|u_k\|} \\
&\vdots & &\vdots
\end{aligned}$$

We claim that $\operatorname{span}_F\{v_1, \dots, v_k\} = \operatorname{span}_F\{w_1, \dots, w_k\}$ and $\{w_1, \dots, w_k\}$ is an orthonormal set, for each $1 \le k \le r$. It is trivial when $k = 1$. Suppose this assertion is true for some $k = m < r$, then $\langle u_{m+1}, w_i\rangle = \langle v_{m+1}, w_i\rangle - \langle v_{m+1}, w_i\rangle = 0$ for $i \le m$. Also, $v_{m+1} \notin \operatorname{span}_F\{w_1, \dots, w_m\} = \operatorname{span}_F\{v_1, \dots, v_m\}$, since $\{v_1, v_2, \dots, v_r\}$ is linearly independent. We thus have $u_{k+1} \neq 0$, this completes the proof by mathematical induction on k. □

Corollary.

1. If $(V, \langle\ ,\ \rangle)$ is a finite dimensional inner product space over F, then an orthonormal basis exists.

2. Let Ω be a positive definite matrix. From the remark of Definition 15, Ω defines an inner product on $V = F^n$. Let P be an invertible matrix such that $Pe_i = w_i$, where $\{e_1, \dots, e_n\}$ is the standard basis of V and $\{w_1, \dots, x_n\}$ is one orthonormal basis of V with respect to the inner product defined by Ω. Then, Theorem 13 asserts

   $$I_n = P^{\mathrm{t}} \cdot \Omega \cdot \overline{P} \implies \Omega = {P^{-1}}^{\mathrm{t}} \cdot \overline{P^{-1}}.$$

   Let $Q = {P^{-1}}^{\mathrm{t}}$, then we conclude

   $$\Omega = Q \cdot Q^*.$$

> For each positive definite matrix $\Omega \in M_n(F)$, there is an invertible matrix $Q \in M_n(F)$ such that $\Omega = Q \cdot Q^*$.

Recall that in Theorem 19 we have shown the existence of $\operatorname{Proj}_W(x)$ when W is a subspace of finite dimensional vector space V. In fact, we can derive the same result but using a weaker condition.

Theorem 23 (orthogonal projection revisited)**.** *Let* $(V, \langle\ ,\ \rangle)$ *be an inner product space. (It could be infinite dimensional.) Let* $W \subset V$ *be a subspace with finite dimension. Then,* $\operatorname{Proj}_W(x)$ *exists*

uniquely. In fact,

$$\mathrm{Proj}_W(x) = \sum_{i=1}^{n} \langle x, w_i \rangle \cdot w_i,$$

where $\{w_1, w_2, \dots, w_n\}$ *is an orthogonal basis of* W*.*

Proof. We first show that $\left\langle x - \mathrm{Proj}_W(x), w \right\rangle = 0$, for all $w \in W$. Note that

$$\left\langle x - \mathrm{Proj}_W(x), w_i \right\rangle = \langle x, w_i \rangle - \langle x, w_i \rangle = 0,$$

for all $1 \le i \le n$. It remains to show $\mathrm{Proj}_W(x)$ is unique. Let $y \in W$ such that $x - y \in W^\perp$, then

$$\begin{aligned}
\left\| \mathrm{Proj}_W(x) - y \right\|^2 &= \left\langle \mathrm{Proj}_W(x) - y, \mathrm{Proj}_W(x) - y \right\rangle \\
&= \left\langle \mathrm{Proj}_W(x) - x + x - y, \mathrm{Proj}_W(x) - y \right\rangle \\
&= \left\langle \mathrm{Proj}_W(x) - x, \mathrm{Proj}_W(x) - y \right\rangle + \left\langle x - y, \mathrm{Proj}_W(x) - y \right\rangle \\
&= 0 + 0 = 0\,.
\end{aligned}$$

□

We now generalize the idea of orthogonal projection to the case when the subspace W is not given.

Definition 24 (Projection)**.** Let V be an inner product space over F, and let $T : V \to V$ be a linear transformation.

1. We say T is a projection if $T^2 = T$.
2. We say T is an orthogonal projection if $T^2 = T$ and $(\mathrm{Im}T)^\perp = \ker T$.

Remark. Let $T : V \to V$ be an orthogonal projection defined as above. Then, $T(v) = \mathrm{Proj}_W(v)$, where $W := \mathrm{Im}T$.

2.3 Hilbert space

In the previous text, lots of properties of inner product spaces only hold when the space is finite dimensional. This subsection we shall introduce a kind of inner product space that act like a finite dimensional inner product space.

Definition 25 (Hilbert space)**.** Let $(V, \langle\ ,\ \rangle)$ be an inner product space. The norm $\|\cdot\|$ induces a metric d on V. V is said to be a Hilbert space, if (V, d) is a complete metric space in the sense that every Cauchy sequence converges. A subspace $W \subset V$ is closed if W is a Hilbert subspace.

Remark. In analysis, "closedness" of a subspace W means that every convergent sequence in W converges to a point in W. This definition coincides the above definition.

Theorem 26 (Existence of orthogonal projection)**.** *Let $(V, \langle\ ,\ \rangle)$ be a Hilbert space and let $W \subset V$ be a closed subset. Then,* $\mathrm{Proj}_W(x)$ *exists uniquely.*

Proof. Let $d := \inf_{w \in W} \|w - x\|$. We claim that there exist a vector $y_0 \in W$ such that $\|y_0 - x\| = d$. By the definition of infimum, there exist y_n such that

$$d \leq \|y_n - x\| < d + \frac{1}{n}.$$

We first show that (y_n) is a Cauchy sequence. Given $\epsilon > 0$. Let $N \in \mathbb{N}$ large enough so that

$$\frac{8d}{N} + \frac{4}{N^2} < \epsilon.$$

By the parallelogram law, we have

$$\begin{aligned}
\|y_n - y_m\|^2 &= 2(\|y_n - x\|^2 + \|y_m - x\|^2) - \|y_n + y_m - 2x\|^2 \\
&< 2\left(\left(d + \frac{1}{n}\right)^2 + \left(d + \frac{1}{m}\right)\right) - 4\left\|\frac{y_n + y_m}{2} - x\right\|^2 \\
&< 4\left(d + \frac{1}{N}\right)^2 - 4d^2 = \frac{8d}{N} + \frac{4}{N^2} < \epsilon,
\end{aligned}$$

where $n, m \geq N$. Hence, (y_n) is a Cauchy sequence. Suppose $y_n \to y_0$, then $\|y_0 - x\| = d$. We now show that $p = x - y_0 \in W^\perp$. Let us introduce two parameters $t \in F$ and $w \in W$, then we have

$$\begin{aligned}
& \|p - t \cdot w\|^2 = \|x - y_0 - t \cdot w\|^2 \geq d^2 \\
\implies \quad & \|p\|^2 + t^2 \cdot \|w\|^2 - 2\Re\left(\bar{t} \cdot \langle p, w\rangle\right) \geq d^2 \qquad (3) \\
\implies \quad & t^2 \cdot \|w\|^2 - 2\Re\left(\bar{t} \cdot \langle p, w\rangle\right) \geq 0.
\end{aligned}$$

If $\langle p, w\rangle \neq 0$, then $\langle p, w\rangle = r \cdot \exp(i\theta)$ for some $r > 0$. We plug in $t = \epsilon \cdot \exp(i\theta)$ to (3), for small enough $\epsilon > 0$. Then,

$$\epsilon^2 \|w\|^2 \geq 2 \cdot \Re(\epsilon r),$$

which fail to be true when ϵ is small enough. Therefore, $y_0 = \lim y_n = \mathrm{Proj}_W(x)$. □

Next, we introduce the concept of bounded linear functional.

Definition 27 (Bounded linear functional)**.** Let $(V, \langle\ ,\ \rangle)$ be a Hilbert space over F. A linear functional $\ell : V \to F$ is said to be bounded if there exists $M > 0$ such that

$$|\ell(v)| \leq M \cdot \|v\|,$$

for all $v \in V$. The set of all bounded linear functional on V is denoted by $V^\vee_{\mathrm{bdd}}$. In fact, we can similarly define the concept of bounded linear transformation.

Remark.

1. Any bounded linear functional is a continuous function, with respect to the norm of V and metric on F.

2. Any finite dimensional inner product space V is a Hilbert space, moreover, $V^{\vee}_{\text{bdd}} = V^{\vee}$.

Theorem 28 (Riesz representation theorem)**.** *Let $(V, \langle\ ,\ \rangle)$ be a Hilbert space, and let $\ell \in V^{\vee}_{\text{bdd}}$ be a bounded linear functional, then there exist $y \in V$, such that*

$$\ell(x) = \langle x, y \rangle,$$

for all $x \in V$.

Proof. Let ℓ be a bounded linear functional. Then, $N = \ker \ell$ is a closed subspace of V. (Recall that the preimage under a continuous function of a closed set is closed.) If N is V, then $\ell = 0$, and we can take $y = 0$. Now, we assume that $N \subsetneq V$, it follows from Theorem 26 that there exists $v \in N^{\perp}$. (Hence $\ell(v) \neq 0$.) Consider a function $\alpha(x) = \ell(x)/\ell(v)$, for all $x \in V$. Then,

$$\begin{aligned}
&\ell(x) = \alpha(x) \cdot \ell(v) \\
\implies &\ell(x - \alpha \cdot v) = 0 \\
\implies &x - \alpha \cdot v \in N \\
\implies &\langle x - \alpha \cdot v, v \rangle = 0 \\
\implies &\langle x, v \rangle = \alpha \cdot \langle v, v \rangle \\
\implies &\ell(x) = \langle x, y \rangle, \text{ where } y = \frac{\overline{\ell(v)}}{\|v\|^2} \cdot v.
\end{aligned}$$

□

2.4 Adjoint linear transformation

Definition 29 (Adjoint linear transformation)**.** Let $(V, \langle\ ,\ \rangle)$ and $(W, \langle\ ,\ \rangle)$ be two inner product spaces over F and let $T : V \to W$ be a linear transformation. We define the adjoint of T is the transformation $T^* : W \to V$ such that:

$$\langle T^*(w), v \rangle = \langle w, T(v) \rangle,$$

for all $v \in V$ and $w \in W$.

We now show that T^* exists uniquely if both V and W are finite dimensional.

Theorem 30. *Let V and W be two finite dimensional inner product spaces and let $T : V \to W$ be a linear transformation. Then, T^* exists uniquely.*

Proof. By Theorem 22, there exist orthonormal bases of V and W, say $\mathcal{A} = \{v_1, \dots, v_n\}$ and $\mathcal{B} = \{w_1, \dots, w_m\}$, respectively. Let $[T]_{\mathcal{A},\mathcal{B}} = A = (a_{ij})_{m \times n}$. We now assume T^* exists, and let $[T^*]_{\mathcal{B},\mathcal{A}} = (b_{ij})_{n \times m}$. Then,

$$\begin{aligned}
&\left\langle T^*(w_i), v_j \right\rangle = \left\langle w_i, T(v_j) \right\rangle \\
\implies &\left\langle \sum_{k=1}^{n} b_{ki} \cdot v_k, v_j \right\rangle = \left\langle w_i, \sum_{l=1}^{m} a_{lj} \cdot w_l \right\rangle \\
\implies &b_{ji} = \overline{a_{ij}}.
\end{aligned}$$

This shows the uniqueness of T^*. In fact, this also shows the existence of T^*, since we can define:

$$T^* : W \to V$$
$$[w]_{\mathcal{B}} \mapsto A^* \cdot [w]_{\mathcal{B}},$$

where $[w]_{\mathcal{B}}$ denote the coordinate vector of w with respect to the basis $\mathcal{B}$. The calculations above implies T^* meets the condition of adjoint linear transformation. □

However, the adjoint of an operator is not always exist, especially in infinite dimensional inner product space. The next theorem asserts that some operators on Hilbert space has an adjoint. We shall first introduce the concept of bounded linear transformation.

Definition 31 (Bounded linear transformation)**.** Let $T : V \to W$ be a linear transformation between two normed space. Then T is said to be bounded if there exists $M > 0$ such that

$$\|T(v)\|_W \leq M \cdot \|v\|_V , \text{ for all } v \in V.$$

Theorem 32 (existence of adjoint operators on Hilbert space)**.** *Let V be a Hilbert space. (Recall Definition 25.) Let $T : V \to V$ be a bounded linear operator. Then, T^*, the adjoint of T, exists.*

Proof. This is a corollary of the "Riesz representation theorem". For each $x \in V$, consider linear functionals:

$$\ell_{T,x}(y) = \langle T(y), x \rangle , \quad y \in V.$$

It is easy to check that $\ell_{T,x}$ is linear. We claim that if T is bounded then $\ell_{T,x}$ is bounded. Note that

$$\left|\ell_{T,x}(y)\right| = \left|\langle T(y), x \rangle\right| \leq \left\|T(y)\right\| \|x\| \leq M \left\|y\right\| \|x\| .$$

Thus, $\ell_{T,x}$ is bounded. It follows from Theorem 28 that there exists a unique $z \in V$ such that

$$\ell_{T,x}(y) = \langle y, z \rangle = \langle T(y), x \rangle , \text{ for all } y \in V$$

We define $T^*(x) := z$. It is easy to verify that T^* is a linear transformation. □

Theorem 33. *Let V, W be inner product spaces over F, and let T_1, T_2 and T be linear transformations from V to W. Suppose T_1^*, T_2^* and T^* exist. Then, the following properties hold:*

1. $(T_1 + T_2)^* = T_1^* + T_2^*$.
2. $(\alpha \cdot T)^* = \overline{\alpha} \cdot T^*$, *for* $\alpha \in F$.
3. *Let U be an inner product space and let $S : W \to U$ be a linear transformation with the adjoint exists. Then,* $(S \circ T)^* = T^* \circ S^*$.
4. $T^{**} = T$.

The proof is very straightforward, so we omit it.

Theorem 34. *Let $T : V \to W$ be a linear transformation between two "finite dimensional" inner product spaces. Then,*

1. $(\mathrm{Im}T)^{\perp} = \ker(T^*)$.

2. $(\ker T)^{\perp} = \mathrm{Im}(T^*)$.

Proof. To show the first assertion, suppose $w \in (\mathrm{Im}T)^{\perp}$, namely,

$$\begin{aligned} & \langle w, T(v)\rangle = 0, \text{ for all } v \in V. \\ \iff \quad & \langle T^*(w), v\rangle = 0, \text{ for all } v \in V. \\ \iff \quad & T^*(w) = 0. \\ \iff \quad & w \in \ker(T^*). \end{aligned}$$

Similarly, for the second assertion. we assume that $v \in \mathrm{Im}(T^*)$, then $v = T^*(w)$ for some $w \in W$. Note that

$$\langle v, x\rangle = \langle T^*(w), x\rangle = \langle w, T(x)\rangle = 0, \text{ for all } x \in \ker T.$$

Thus, we conclude that $\mathrm{Im}(T^*) \subset (\ker T)^{\perp}$. By the dimensional formulas, we get $\mathrm{Im}(T^*) = (\ker T)^{\perp}$. □

Definition 35 (Unitary linear transformation (operator))**.** Let $T : V \to W$ be a linear transformation between two inner product spaces (probably infinite dimensional). T is called unitary if

$$\langle T(v_1), T(v_2)\rangle = \langle v_1, v_2\rangle,$$

for all $v_1, v_2 \in V$.

The next theorem gives a characterization of unitary operators.

Theorem 36. *Given a linear transformation $T : V \to W$ between two finite dimensional inner product spaces. Then the following statements are equivalent:*

1. *T is unitary.*

2. *$\|T(v)\| = \|v\|$, for all $v \in V$.*

3. *$T^* \circ T = \mathrm{Id}_V$.*

4. *T sends the orthonormal basis to an orthonormal set.*

Proof.
(1) $\Longrightarrow$ (2): Obvious.
(2) $\Longrightarrow$ (1): Consider $\left\|T(x+y)\right\|^2 = \left\|x+y\right\|^2$.

$$\begin{aligned} & \langle T(x), T(y)\rangle + \langle T(y), T(x)\rangle = \langle x, y\rangle + \langle y, x\rangle \\ \Longrightarrow\ & \Re\Big(\langle T(x), T(y)\rangle\Big) = \Re\Big(\langle x, y\rangle\Big). \end{aligned} \tag{4}$$

If $F = \mathbb{R}$, then (4) shows that $\langle T(x), T(y)\rangle = \langle x, y\rangle$. If $F = \mathbb{C}$, then plugging in $y \mapsto i \cdot y$ to equation (4) gives

$$\Re\Big((-i)\cdot\langle T(x), T(y)\rangle\Big) = \Re\Big((-i)\cdot\langle x, y\rangle\Big).$$

Together with equation 4 indicate that T is unitary.
(3) $\iff$ (1): T is unitary if and only if

$$\begin{aligned} & \langle T(x), T(y)\rangle = \langle x, y\rangle \text{ , for all } x, y \in V \\ \iff \quad & \langle T^*T(x), y\rangle = \langle x, y\rangle \text{ , for all } x, y \in V \\ \iff \quad & \langle (T^*T - \mathrm{Id}_V)(x), y\rangle = 0, \text{ for all } x, y \in V \\ \iff \quad & (T^*T - \mathrm{Id}_V) \equiv 0. \end{aligned}$$

(1) $\iff$ (4): Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be an orthonormal basis of V. Then,

$$\left\langle T(v_i), T(v_j)\right\rangle = \left\langle v_i, v_j\right\rangle = \begin{cases} 1, \text{ if } i \neq j \\ 0, \text{ if } i = j \end{cases}.$$

Thus, $T(\mathcal{A}) = \{T(v_1), T(v_2), \dots, T(v_n)\}$ is an orthonormal set.

(4) $\iff$ (1): Let $x, y \in V$ be two arbitrary vector in V. Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be an orthonormal basis of V. Assume

$$x = \sum_{i=1}^{n} \alpha_i \cdot v_i, \quad y = \sum_{i=1}^{n} \beta_i \cdot v_i.$$

Then,

$$\langle T(x), T(y)\rangle = \left\langle T(\sum_{i=1}^{n} \alpha_i \cdot v_i), T(\sum_{i=1}^{n} \beta_i \cdot v_i)\right\rangle = \sum_{i=1}^{n} \alpha_i \cdot \overline{\beta_i} = \langle x, y\rangle .$$

□

2.5 Spectral theory of normal operators

Definition 37 (Self-adjoint and normal operator)**.** Let $T : V \to V$ be a linear operator on an inner product space V.

1. We say T is self-adjoint, if $T = T*$.
2. We say T is normal, if $T \circ T^* = T^* \circ T$.

Remark. A linear operator $T : V \to V$ is unitary if and only if $T^* = T^{-1}$. (Assume that V is finite dimensional.) Thus, unitary operators and self-adjoint operators are normal.

In the rest of this subsection, if not specifically mentioned, V denotes the finite dimensional inner product space over F ($\mathbb{R}$ or $\mathbb{C}$.)

Theorem 38. *Given $T : V \to V$, a linear operator on finite dimensional space V. The the following statements are equivalent.*

1. *T is normal.*
2. *$\|T(v)\| = \|T^*(v)\|$, for all $v \in V$.*

Proof.
(1) $\implies$ (2): Note that

$$\langle T(v), T(v)\rangle = \langle T^*T(v), v\rangle = \langle TT^*(v), v\rangle = \langle T^*(v), T^*(v)\rangle .$$

(2) $\implies$ (1): Consider $\left\|T(x+y)\right\|^2 = \left\|T^*(x+y)\right\|^2$ (and $\left\|T(x+i\cdot y)\right\|^2 = \left\|T^*(x+i\cdot y)\right\|^2$ if $F = \mathbb{C}$.) Expanding both equations gives

$$\langle T^*T(x), y\rangle = \langle TT^*(x), y\rangle , \text{ for all } x, y \in V.$$

Thus, $T \circ T^* \equiv T^* \circ T$. □

Corollary. Let $T : V \to V$ be a linear operator on a finite dimensional vector space V. Suppose T is normal, and v is an eigenvector of T with eigenvalue λ. Then, v is an eigenvector of T^* with eigenvalue $\overline{\lambda}$.

Proof. Since T is normal, $S = T - \lambda \cdot \mathrm{Id}_V$ is normal. (In fact, $p(T)$ is normal, for all $p(x) \in F[x]$.) We have $Sv = 0$. From Theorem 38, we have $\|S^*v\| = \|Sv\| = 0$. Hence, v is in the kernel of $S^* = T^* - \overline{\lambda} \cdot \mathrm{Id}_V$. This completes the proof. □

We now prove an useful lemma.

Lemma 3. Let T be a linear operator on V, such that T^* exists. (We have assumed nothing about whether it is normal.) Then,

$$\ker T^*T = \ker T.$$

Proof. Obviously, $\ker T \subset \ker T^*T$. It suffices to show that $\ker T^*T \subset \ker T$. Let $v \in \ker T^*T$, then,

$$\begin{aligned} T^*T(v) = 0 &\implies \langle T^*T(v), v\rangle = 0 \\ &\implies \langle T(v), T(v)\rangle = 0 \\ &\implies \|T(v)\| = 0 \\ &\implies T(v) = 0. \end{aligned}$$

□

Theorem 39 (Semi-simplicity of normal operators)**.** *Suppose T is a normal operator on V. If $T^n \equiv 0$, for some $n \geq 1$. Then $T \equiv 0$.*

Proof. Let $S = T^*T$. By Lemma 3, it suffices to show $\ker S = V$. Since $T^n = 0$, we have $S^n = 0$. (T^* and T commute.) We may enlarge n so that $n = 2^k$ for some $k \in \mathbb{N}$. Note that

$$\left\|S^{2^{k-1}}v\right\|^2 = \left\langle S^{2^{k-1}}v, S^{2^{k-1}}v\right\rangle = \left\langle \left(S^{2^{k-1}}\right)^* S^{2^{k-1}}v, v\right\rangle = \left\langle S^{2^k}v, v\right\rangle = 0.$$

Repeating this process gives us $S = 0$. □

Before we introduce the next theorem (Theorem 40), we shall first prove another useful result.

Lemma 4. Let V be an inner product space over F, and let $T : V \to V$ be a normal operator on V. Suppose $p(x)$ and $q(x)$ are polynomials in F with no common roots. Then,

$$\ker(p(T)) \perp \ker(q(T)),$$

that is, $\langle v, w\rangle = 0$, for all $v \in \ker(p(T))$ and $w \in \ker(q(T))$.

Proof. Since p, q have no common roots, there exist $A, B \in F[x]$, such that

$$A(x)p(x) + B(x)q(x) = 1.$$

Let $v \in \ker(p(T))$ and $w \in \ker(q(T))$. We have $B(T)q(T)(v) = v$. Thus,

$$\langle v, w\rangle = \langle B(T)q(T)(v), w\rangle = \langle q(T)B(T)v, w\rangle = \langle B(T)v, q(T)^*(w)\rangle \overset{(\spadesuit)}{=} \langle B(T)v, 0\rangle = 0.$$

($\spadesuit$) is true since:

$$\begin{aligned} w \in \ker(q(T)) &\implies \left\|q(T)(w)\right\| = 0 \\ &\implies \left\|q(T)^*(w)\right\| = 0 \\ &\implies q(T)^*(w) = 0. \end{aligned}$$

□

Theorem 40. *Let $(V, \langle\ ,\ \rangle)$ be an finite dimensional inner product space over $\mathbb{C}$. Let $T : V \to V$ be a normal operator on V. Then, T is diagonalizable. Moreover,*

$$V = \bigoplus_{i=1}^{s} E_{\lambda_i} = E_{\lambda_1} \oplus E_{\lambda_2} \oplus \cdots \oplus E_{\lambda_s}$$

is the orthogonal decomposition of eigenspaces of V. Recall that E_{λ_i} is the eigenspace that which has eigenvalue λ.

Here we give two proofs.

Proof. Let $\mathrm{ch}_T(x)$ be the characteristic polynomial of T. The fundamental theorem of algebra asserts that $\mathrm{ch}_T(x)$ splits completely, that is,

$$\mathrm{ch}_T(x) = \prod_{i=1}^{s} (x - \lambda_i)^{n_i}.$$

Then, we have learnt that $V = \bigoplus_{i=1}^{s} W_i$ in the theory of Jordan forms, where

$$W_i = \ker(T - \lambda_i \cdot \mathrm{Id}_V)^{n_i}.$$

Consider $T|_{W_i}$ on $(W_i, \langle\ ,\ \rangle|_{W_i \times W_i})$. Note that $T|_{W_i}$ is normal and that $(T|_{W_i} - \lambda_i \cdot \mathrm{Id}_{W_i})^{n_i} = 0$. By Theorem 39, we conclude $T|_{W_i} - \lambda_i \cdot \mathrm{Id}_{W_i} = 0$. This implies

$$W_i = \ker(T - \lambda_i \cdot \mathrm{Id}_V)^{n_i} = \ker(T - \lambda_i \cdot \mathrm{Id}_V) = E_{\lambda_i}.$$

It remains to show that each E_{λ_i} is orthogonal to each other. It follows by Lemma 4. □

Here is an alternative proof using mathematical induction.

Proof. Let $\lambda \in \mathbb{C}$ be an eigenvalue of T. Then,

$$E_\lambda = \{v \in V : T(v) = \lambda \cdot v\} \neq \{0\}.$$

Decompose V into $E_\lambda \oplus E_\lambda^\perp$. ($V$ is finite dimensional.) We claim that $E_\lambda^\perp$ is a T-invariant subspace. Let $x \in E_\lambda^\perp$ and $v \in E_\lambda$. Then,

$$\langle T(x), v\rangle = \langle x, T^*(v)\rangle \overset{(\spadesuit)}{=} \left\langle x, \overline{\lambda} v\right\rangle = \lambda \langle x, v\rangle = 0.$$

The equality ($\spadesuit$) holds because of Corollary 2.5. On the other hand,

$$\dim E_\lambda^\perp < \dim V.$$

By induction, $T|_{E_\lambda^\perp}$ is diagonalizable and

$$E_\lambda^\perp = \bigoplus_i E_{\lambda_i}.$$

This completes the proof. □

However, Theorem 40 is not true for inner product space over $\mathbb{R}$. But we have the following theorem.

Theorem 41. *Let V be a finite dimensional inner product space over $\mathbb{R}$, and let $T : V \to V$ be a self-adjoint operator on V. Then, T is diagonalizable. Moreover,*

$$V = \bigoplus_{i=1}^{s} E_{\lambda_i},$$

and $E_{\lambda_i} \perp E_{\lambda_j}$ if $i \neq j$.

Proof. In view of the proofs of Theorem 40, it suffices to show that $\mathrm{ch}_T(x)$ splits completely in $\mathbb{R}$. Choose an orthonormal basis $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ of V. Define a matrix

$$A := [T]_{\mathcal{A}} = (a_{ij})_{n\times n}.$$

Then, it is well-known that

$$[T^*]_{\mathcal{A}} = A^*.$$

Hence $A^* = A$ since T is self-adjoint. Now, assume $\lambda \in \mathbb{C}$ is an eigenvalue of T. Then, there exists $x \in \mathbb{C}^n \setminus \{0\}$ (column vector) such that

$$Ax = \lambda \cdot x.$$

Consider

$$\overline{\lambda}(x^* \cdot x) = (Ax)^* \cdot x = x^* \cdot A^* \cdot x = x^* \cdot A \cdot x = \lambda \cdot (x^* \cdot x).$$

This indicates

$$\lambda \cdot \|x\|^2 = \overline{\lambda} \cdot \|x\|^2 \implies \lambda \in \mathbb{R}.$$

□

Corollary. Let $A \in M_n(\mathbb{C})$ be a complex normal matrix, that is,

$$A^* \cdot A = A \cdot A^*.$$

Then, there exists an invertible matrix $P \in M_n(\mathbb{C})$ such that:

1. $P \cdot P^* = I_n$.
2. $P^{-1}AP$ is diagonal.

Proof. Let $V = \mathbb{C}^n$ be an inner product space equipped with the standard inner product structure. Let $T : V \to V$ be the operator defined by

$$v \mapsto A \cdot v.$$

Then, the standard basis is orthonormal and hence $A^* = A$ is equivalent to T is self-adjoint. It follows from Theorem 40 that

$$V = \bigoplus_{i=1}^{s} E_{\lambda_i}$$

is a orthogonal decomposition. For each E_{λ_i}, we choose an orthonormal basis

$$\mathcal{A}_i = \left\{v_{i1}, \dots, v_{in_i}\right\}.$$

Then,

$$\mathcal{A} = \bigsqcup_{i=1}^{s} \mathcal{A}_i = \mathcal{A}_1 \sqcup \mathcal{A}_2 \sqcup \cdots \sqcup \mathcal{A}_s$$

is an orthonormal basis. (Because $E_{\lambda_i} \perp E_{\lambda_j}$.) Let P be the matrix sends the standard basis to $\mathcal{A}$. By Theorem 36, we conclude that $P \cdot P^* = P^* \cdot P = I_n$. Also, it is easy to see

$$P^{-1}AP = \begin{pmatrix} \lambda_1 I_{n_1} & 0 & \cdots & 0 \\ 0 & \lambda_2 I_{n_2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_s I_{n_s} \end{pmatrix}.$$

This completes the proof. □

Similarly, one can prove the following result:

Corollary. Let $A \in M_n(\mathbb{R})$ be a real matrix such that $A^{\mathsf{t}} = A$. Then, there exists an invertible matrix $P \in M_n(\mathbb{R})$ such that:

1. $P^{\mathsf{t}} \cdot P = P \cdot P^{\mathsf{t}} = I_n$.
2. $P^{-1}AP$ is diagonal.

Corollary. Let T be a self-adjoint operator on inner product space V over F. Then, there exists $\lambda_i \in \mathbb{R}$ such that

$$T(v) = \lambda_1 \cdot \mathrm{Proj}_{E_{\lambda_1}}(v) + \lambda_2 \cdot \mathrm{Proj}_{E_{\lambda_2}}(v) + \cdots + \lambda_s \cdot \mathrm{Proj}_{E_{\lambda_s}}(v).$$

In Theorem 41, we show that every self-adjoint operator on vector space over $\mathbb{R}$ is diagonalizable. However, we do not deal with all normal operators. The next theorem is discussing operators over real inner product space.

Theorem 42. *Let $A \in M_n(\mathbb{R})$ be a real normal matrix, that is,*

$$A^{\mathrm{t}} \cdot A = A \cdot A^{\mathrm{t}}.$$

Then, there exists an invertible matrix $P \in M_n(\mathbb{R})$ such that:

1. $P \cdot P^{\mathrm{t}} = P^{\mathrm{t}} \cdot P = I_n$.
2. $P^{-1}AP = (\bigoplus_{i=1}^{s} \lambda_i I_{n_i}) \oplus (\bigoplus_{j=1}^{r} D_j^{\oplus m_j})$, *where all $\lambda_i \in \mathbb{R}$, and all D_j have the form:*

$$\begin{pmatrix} \alpha_j & \beta_j \\ -\beta_j & \alpha_j \end{pmatrix}.$$

Remark. Here, we have a little abuse of notation. We write $A \oplus B$ to represent

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

if both A and B are square matrices. Also, we write $P^{\oplus k}$ to mean $\bigoplus_{i=1}^{k} P = P \oplus P \oplus \cdots \oplus P$, for square matrix P.

Before we start proving this theorem, we shall first prove some useful lemmas.

Lemma 5. Let V be an inner product space over $\mathbb{R}$, and let $T : V \to V$ be a normal operator, such that

$$S^2 = -\mathrm{Id}_V.$$

Let $v_1 \in V \setminus \{0\}$ and $v_2 = S(v_1)$. Then,

$$S^*(v_1) = -v_2, \quad S^*(v_2) = v_1, \quad \langle v_1, v_2 \rangle = 0, \quad \|v_1\| = \|v_2\|.$$

Proof. Consider

$$\begin{aligned}
&\|S^*v_1 + v_2\|^2 + \|S^*v_2 - v_1\|^2 \\
&= \langle S^*v_1, S^*v_1 \rangle + \langle S^*v_1, v_2 \rangle + \langle v_2, S^*v_1 \rangle + \langle v_2, v_2 \rangle \\
&\qquad + \langle S^*v_2, S^*v_2 \rangle - \langle S^*v_2, v_1 \rangle - \langle v_1, S^*v_2 \rangle + \langle v_1, v_1 \rangle \\
&= \langle Sv_1, Sv_1 \rangle + 2 \cdot \langle Sv_2, v_1 \rangle + \langle v_2, v_2 \rangle + \langle Sv_2, Sv_2 \rangle - 2 \cdot \langle Sv_1, v_2 \rangle + \langle v_1, v_1 \rangle \\
&= \|Sv_1 - v_2\|^2 + \|Sv_2 + v_1\|^2 = 0.
\end{aligned}$$

This prove the first two assertion. Note that

$$\langle v_1, v_2 \rangle = \langle v_1, Sv_1 \rangle = \langle S^*v_1, v_1 \rangle = \langle -v_2, v_1 \rangle = -\langle v_1, v_2 \rangle$$

and that

$$\|v_2\|^2 = \langle v_2, v_2 \rangle = \langle Sv_1, v_2 \rangle = \langle v_1, S^*v_2 \rangle = \langle v_1, v_1 \rangle = \|v_1\|^2.$$

□

From Lemma 5, we conclude that:

Continuing from the above definition, let

$$w_1 = \frac{v_1}{\|v_1\|}, \quad w_2 = \frac{v_2}{\|v_2\|}.$$

Then, $\{w_1, w_2\}$ is an orthonormal set. Moreover, $W := \text{span}_{\mathbb{R}}\{w_1, w_2\}$ is S-invariant and S^*-invariant.

$$\left[S|_W\right]_{\{w_1,w_2\}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Lemma 6. Let $T : V \to V$ be a normal operator on a finite dimensional inner product space. Suppose

$$\text{ch}_T(x) = \left((x-a)^2 + b^2\right)^m,$$

for some $b \neq 0$. Then, there exists an orthonormal basis $\mathcal{A}$ such that

$$[T]_{\mathcal{A}} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{\oplus m}.$$

Proof. Let $S = (T-a)/b$. Then, by Lemma 5, we have an orthonormal set $\mathcal{A}_1 = \{w_1, w_2\}$. Define $W_1 = \text{span}_{\mathbb{R}}\{w_1, w_2\}$. Then,

$$\left[S|_{W_1}\right]_{\{w_1,w_2\}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

That indicates that

$$\left[T|_{W_1}\right]_{\{w_1,w_2\}} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

We now claim that $W_1^\perp$ is a S-invariant subspace. Let $v \in W_1^\perp$ and $w \in W_1$, then

$$\langle Sv, w\rangle = \langle v, S^*w\rangle = 0,$$

since W_1 is also a S^*-invariant subspace. Similarly, we have an orthonormal set $\mathcal{A}_2 \subset W_1^\perp$ such that

$$\left[S|_{W_2}\right]_{\mathcal{A}_2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where W_2 is the subspace generated by $\mathcal{A}_2$. Also, $(W_1 \oplus W_2)^\perp$ is a S-invariant. Continuing this process give s

$$V = \bigoplus_{i=1}^{s} W_i,$$

each W_i is spanned by an orthonormal set $\mathcal{A}_i$ and

$$\left[S|_{W_i}\right]_{\mathcal{A}_i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Let $\mathcal{A} = \bigsqcup \mathcal{A}_i$, then

$$[T]_{\mathcal{A}} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{\oplus m}.$$

□

Lemma 7. Let $T : V \to V$ be a normal operator on a finite dimensional vector space V over $\mathbb{R}$. Suppose $\mathrm{m}_T(x) = \prod_{i=1}^{s} f_i$, where f_i are all irreducible. Then, f_i are all distinct.

Proof. Suppose not, then there exists an irreducible polynomial $f \in \mathbb{R}[x]$ such that $f = f_i$ for more than one i. Let us consider $W = \ker f^n(T)$, then W is a $f(T)$-invariant subspace. Note that $f(T)$ is normal on W and $f(T)^n \equiv 0$ on W. Thus, from Theorem 39, we conclude that

$$\ker f(T) = \ker f^n(T),$$

which leads to a contradiction. □

Proof of Theorem 42. From Lemma 7, we assume that

$$\mathrm{m}_T(x) = \left(\prod_{i=1}^{s} (x - \lambda_i) \right) \cdot \left(\prod_{j=1}^{r} \left((x - a_j)^2 + b_j^2 \right) \right).$$

From what we have learnt in the theory of Jordan forms,

$$V = \left(\bigoplus_{i=1}^{s} \ker (T - \lambda_i) \right) \oplus \left(\bigoplus_{j=1}^{r} \ker \left((T - a_j)^2 + b_j^2 \right) \right).$$

For simplicity, we define $W_i := \ker (T - \lambda_i)$ and $X_j := \ker \left((T - a_j)^2 + b_j^2 \right)$. It suffices to show that for each j, there exists a basis $\mathcal{A}_j$ such that

$$\left[T|_{X_j} \right]_{\mathcal{A}_j} = D_j^{\oplus m_j},$$

where

$$D_j := \begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix}.$$

This follows from Lemma 6. □

2.6 Applications of spectral theory of normal operators

This subsection is mainly deal with two topics:

1. Structure of orthogonal (unitary) operators.
2. Singular value decomposition (SVD).

In this subsection, we assume that V is a finite dimensional inner product space unless otherwise stated.

Definition 43 (Unitary groups and orthogonal groups)**.** Let V be a finite dimensional inner product space over F.

1. If $F = \mathbb{C}$, we define the unitary group
$$\mathrm{U}(V) = \{T : V \to V \mid T \cdot T^* = T^* \cdot T = \mathrm{Id}_V\}.$$
2. If $F = \mathbb{R}$, we define the orthogonal group
$$\mathrm{O}(V) = \{T : V \to V \mid T \cdot T^* = T^* \cdot T = \mathrm{Id}_V\}.$$

We also define unitary groups and orthogonal groups by matrices. We write:

1. $\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A \cdot A^{\mathrm{t}} = I_n\}$ is the orthogonal group.
2. $\mathrm{U}_n(\mathbb{R}) = \{A \in M_n(\mathbb{C}) : A \cdot A^* = I_n\}$ is the unitary group.

Note that $\mathrm{U}_n(\mathbb{R})$ contains some complex matrices although it contains $\mathbb{R}$ in its "name". We now focus on orthogonal groups.

Definition 44 (Reflection)**.** Let $T : V \to V$ be a linear operator. T is a reflection if there exists a $z \in V$ with $\|z\| = 1$ such that
$$T(x) = x - 2 \cdot \mathrm{Proj}_z(x) = x - 2 \cdot \langle x, z\rangle \cdot z, \text{ for all } x \in V.$$
We also say that T is the reflection over the hyperplane $\mathcal{H} = (\mathbb{R} \cdot z)^{\perp}$.

Remark. Suppose T is a reflection. Let $\mathcal{A}$ be an orthonormal basis of $\mathcal{H}$. Then, $\mathcal{A}' = \{z\} \sqcup \mathcal{A}$ is an orthonormal basis such that
$$[T]_{\mathcal{A}'} = \begin{pmatrix} -1 & 0 \\ 0 & I_{n-1} \end{pmatrix}.$$
This means that there exists a matrix $P \in \mathrm{O}_n(\mathbb{R})$, such that
$$P^{\mathrm{t}}[T]_{\mathcal{B}}P = \begin{pmatrix} -1 & 0 \\ 0 & I_{n-1} \end{pmatrix},$$
where $\mathcal{B}$ is the standard basis. Hence, we can define reflection on $M_n(\mathbb{R})$.

Definition 45. Let $A \in M_n(\mathbb{R})$ be a real matrix. A is a reflection if (and only if) there exist a $P \in \mathrm{O}_n(\mathbb{R})$ such that
$$P^{\mathrm{t}}AP = \begin{pmatrix} -1 & 0 \\ 0 & I_{n-1} \end{pmatrix}.$$

Lemma 8.

1. If $A \in \mathrm{O}_n(\mathbb{R})$ and $\lambda \in \mathbb{R}$ is an eigenvalue of A, then $\lambda = \pm 1$.
2. If $A \in \mathrm{U}_n(\mathbb{R})$ and $\lambda \in \mathbb{C}$ is an eigenvalue of A, then $|\lambda| = 1$.

Proof. Let $V = F^n$. (F is $\mathbb{R}$ or $\mathbb{C}$.) Define the standard inner product $\langle \cdot, \cdot \rangle$ on V, namely,

$$\langle x, y \rangle = y^* \cdot x, \ x, y \text{ are column vectors.}$$

Then, $A \in \mathrm{O}_n(\mathbb{R})$ ($A \in \mathrm{U}_n(\mathbb{R})$) is a unitary operator on $(V, \langle\ ,\ \rangle)$. If $\lambda \in F$ is an eigenvalue of A, then there exists $v \in V \setminus \{0\}$ such that: $Av = \lambda v$

$$\langle v, v \rangle = \langle Av, Av \rangle = \langle \lambda \cdot v, \lambda \cdot v \rangle = \lambda \cdot \overline{\lambda} \cdot \langle v, v \rangle .$$

This implies $\lambda \cdot \overline{\lambda} = 1$. □

Theorem 46 (Cartan-Dieudonné Theorem)**.** *For every $A \in \mathrm{O}_n(\mathbb{R})$, A is a product of reflections.*

Proof. From Theorem 42, we know that $A \in \mathrm{O}_n(\mathbb{R})$ can be written in the form

$$\left(\bigoplus_{i=1}^{s} (\lambda_i) \right) \oplus \left(\bigoplus_{j=1}^{r} D_j \right), \tag{5}$$

where D_j is

$$\begin{pmatrix} a_j & -b_j \\ b_j & a_j \end{pmatrix}, \text{ for some } a_j, b_j \in \mathbb{R}, \ b_j \neq 0.$$

Lemma 8 asserts that $\lambda_i = \pm 1$ in (5). It is easy to see that (by Definition 45) if $m < n$ and $X \in \mathrm{O}_m(\mathbb{R})$ is a reflection, then so is

$$\begin{pmatrix} X & 0 \\ 0 & I_{n-m} \end{pmatrix}.$$

Thus, it suffices to show that each D_j is a product of reflections on $\mathbb{R}^n$. Since each $D_j \in \mathrm{O}_2(\mathbb{R})$, we know that

$$D_j \cdot D_j^{\mathsf{t}} = I_2.$$

Therefore, $a_j^2 + b_j^2 = 1$, let $\theta \in [0, 2\pi)$ such that $a_j = \cos\theta$ and $b_j = \sin\theta$. Note that

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We conclude that D_j is a product of two reflections. □

Next, we are going to discuss the singular value decomposition. We first define the singular decomposition of a matrix $A \in \mathrm{U}_n(\mathbb{R})$.

Definition 47 (Singular value decomposition (S.V.D.))**.** Let $A \in M_{m\times n}(\mathbb{C})$. If there exist $P \in \mathrm{U}_n(\mathbb{R})$ and $Q \in \mathrm{U}_m(\mathbb{R})$ such that

$$Q^* \cdot A \cdot P = \begin{pmatrix} \Sigma & O_{r\times(n-r)} \\ O_{(m-r)\times r} & O_{(m-r)\times(n-r)} \end{pmatrix} = \begin{pmatrix} \Sigma & 0 \\ 0 & 0 \end{pmatrix} \in M_{m\times n}(\mathbb{C}),$$

where O is the zero matrix in $M_{(m-r)\times(n-r)}(\mathbb{C})$ and $\Sigma \in M_r(\mathbb{C})$ is the diagonal matrix

$$\begin{pmatrix} \sigma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_r \end{pmatrix},$$

with $\sigma_i \in \mathbb{R}$ and $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r$. Then,

$$A = Q \cdot \begin{pmatrix} \Sigma & 0 \\ 0 & 0 \end{pmatrix} \cdot P^*$$

is called the singular value decomposition.

Theorem 48 (Singular value decomposition)**.** *Let $A \in M_{m\times n}(\mathbb{C})$, then the singular value decomposition of A exists.*

It is equivalent to prove the following theorem. Although it is not quite trivial that the following theorem implies the singular value decomposition theorem, it is annoying to write it properly, so we omit the details here.

Theorem 49 (Linear transformation version)**.** *Let V, W be two finite dimensional inner product spaces over F ($\mathbb{R}$ or $\mathbb{C}$) and let $T : V \to W$ be a linear transformation. Then, there exist an orthonormal basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ of V such that*

1. *$\{T(v_1), T(v_2), \dots, T(v_r)\}$ is orthogonal.*
2. *$\{T(v_{r+1}), T(v_{r+2}), \dots, T(v_n)\} = 0$.*

Proof. By Theorem 26, the adjoint T^* of T exists. Consider $S := T^* \circ T : V \to V$. Then S is self-adjoint. Applying the spectral theory for self-adjoint operators (Theorem 41 for $F = \mathbb{C}$ or Theorem 40 for $F = \mathbb{C}$), we can find an orthonormal basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ consisting of eigevectors of S. Let λ_i be the eigenvalue of v_i (with respect to the transformation S), then

$$\left\langle T(v_i), T(v_j) \right\rangle = \left\langle T^*T(v_i), v_j \right\rangle = \left\langle S(v_i), v_j \right\rangle = \lambda_i \left\langle v_i, v_j \right\rangle.$$

This gives

$$\begin{cases} T(v_i) \perp T(v_j), \text{ if } i \neq j. \\ \|T(v_i)\|^2 = \lambda_i, \text{ for all } i. \end{cases}$$

This proves the theorem. □

Singular value decomposition generalize the definition of "inverse matrix". We can define the pseudo inverse or the Moore-Penrose inverse.

Definition 50 (Pseudo inverse or Moore-Penrose inverse)**.** Let $A \in M_{m\times n}(\mathbb{C})$. Let the definition of P and Q be the same as in Definition 47. Then, the Moore-Penrose inverse is defined as

$$A^\dagger := P \cdot \begin{pmatrix} \Sigma^{-1} & 0 \\ 0 & 0 \end{pmatrix} \cdot Q^*.$$

We also can define Moore-Penrose inverse of linear transformation.

Definition 51 (Intrinsic definition of Moore-Penrose inverse)**.** Let V, W be two finite dimensional inner product spaces and let $T : V \to W$ be a linear transformation. Then, the Moore-Penrose inverse is the linear transformation $T^\dagger : W \to V$ defined by:

$$T^\dagger(w) = (T|_{(\ker T)^\perp})^{-1} \circ \mathrm{Proj}_{\mathrm{Im}T}(w).$$

Two definitions of the Moore-Penrose inverse aggee with each other. The Moore-Penrose inverse is invented to solve system linear equations.

Theorem 52. *Let V, W be two finite dimensioal inner product space and let $T : V \to W$. Given $b \in W$. Then, $T(x) = b$ has a solution in V if and only if*

$$b = T \cdot T^{\dagger}(b). \tag{6}$$

In addition, in this case, x is a solution if and only if

$$x = T^{\dagger}(b) + (\mathrm{Id}_V - T^{\dagger} \cdot T)(z), \text{ for some } z \in V.$$

Proof. $T(x) = b$ has a solution in V is equivalent to

$$\begin{aligned} b \in \mathrm{Im}T &\iff \mathrm{Proj}_{\mathrm{Im}T}(b) = b \\ &\iff T \circ T^{\dagger}(b) = b, \text{ by Definition 51.} \end{aligned}$$

To see the second assertion of the theorem, it suffices to show:

$$\ker T = \mathrm{Im}\Big(\mathrm{Id}_V - T^{\dagger} \circ T\Big).$$

However, it follows from the definition that $T^{\dagger} \circ T(v) = \mathrm{Proj}_{(\ker T)^{\perp}}(v)$. Thus,

$$\Big(\mathrm{Id}_V - T^{\dagger} \circ T\Big) = \mathrm{Proj}_{\ker T}.$$

This proves the theorem. □

However, the equation is not always has a solution. In general, $T^{\dagger}(b)$ is the best approximation of solutions of $T(x) = b$ in the following sense:

$$\left\| T \circ T^{\dagger}(b) - b \right\| = \min_{x \in V} \|T(x) - b\|.$$

Theorem 53. *Let V, W be two finite dimensional inner product space and let $T : V \to W$ be a linear transformation. Given $b \in W$. Then, $T^{\dagger}(b)$ is the best approximation of solutions of $T(x) = b$.*

Proof. Since $T \cdot T^{\dagger} = \mathrm{Proj}_{\mathrm{Im}T}$, we have $\Big(T \cdot T^{\dagger}(b) - b\Big) \in (\mathrm{Im}T)^{\perp}$. Thus,

$$\begin{aligned} \|T(x) - b\|^2 &= \left\| T(x) - T \cdot T^{\dagger}(b) + T \cdot T^{\dagger}(b) - b \right\|^2 \\ &= \left\| T(x) - T \cdot T^{\dagger}(b) \right\|^2 + \left\| T \cdot T^{\dagger}(b) - b \right\|^2 \\ &\geq \left\| T \cdot T^{\dagger}(b) - b \right\|^2. \end{aligned}$$

The equality holds if $T(x) = T \cdot T^{\dagger}(b)$. □

2.7 Bilinear forms

In the subsection, unless otherwise stated, we assume F is one of the following fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or the finite field $\mathbb{F}_p$, and let V be a finite dimensional vector space over F.

Definition 54. Let F be a field. Let

$$\Xi = \{n \in \mathbb{N} : n \cdot x = 0, \text{ for all } x \in F\}.$$

Then, the characteristic of F is defined as:

$$\operatorname{char}(F) = \begin{cases} \min \Xi & \text{, if } \Xi \neq \varnothing \\ 0 & \text{, otherwise} \end{cases}.$$

Definition 55 (Bilinear form)**.** Let V be a vector space over F. Then, a bilinear form B is a function

$$B : V \times V \to F$$

such that B is component-wise linear. That is, B is a linear function if we fix one variable.

Thus, the inner product on a vector space over $\mathbb{R}$ is a bilinear form. If B is a bilinear form on a finite dimensional vector space V, then it induce two linear maps from V to $V^\vee$.

$$\begin{aligned} l_B : V &\to V^\vee \\ v &\mapsto l_B(v)(w) = B(v, w), \text{ for all } w \in V \\ r_B : V &\to V^\vee \\ v &\mapsto r_B(v)(w) = B(w, v), \text{ for all } w \in V \end{aligned}$$

Conversely, given a linear transformation $f : V \to V^\vee$, f induces two bilinear forms:

$$\begin{aligned} B_f^l(v, w) &:= f(v)(w) \\ B_f^r(v, w) &:= f(w)(v) \end{aligned}$$

This explains there is a bijection between

$$\{\text{all bilinear forms } B : V \times V \to F\} \simeq \operatorname{Hom}_F(V, V^\vee).$$

We now fix a basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ of V. We get an isomorphism

$$\begin{aligned} \{\text{all bilinear forms } B : V \times V \to F\} &\longleftrightarrow M_n(F) \\ B &\longleftrightarrow \Omega_{B,\mathcal{B}} = \left(B(v_i, v_j)\right). \end{aligned}$$

Similar to what we have shown in the theory of inner product space, if we change the basis to $\mathcal{A}$, then

$$\Omega_{B,\mathcal{A}} = P^{\mathrm{t}} \cdot \Omega_{B,\mathcal{B}} \cdot P,$$

where P is the matrix sends $\mathcal{B}$ to $\mathcal{A}$.

Recall that we have defined the (external) direct sum of two vector spaces in Definition 20. For two vector spaces V, W with bilinear forms B_v, B_w respectively, we can defined a bilinear form B on $V \oplus W$, defined by

$$B((v_1, w_1), (v_2, w_2)) := B_v(v_1, v_2) + B_w(w_1, w_2),$$

and we often write $B = B_v \oplus B_w$. This definition of the direct sum of bilinear forms agrees with the definition of internal direct sum in the following sense:

Let (V, B) be a vector space with a bilinear form. W_1 and W_2 are subspaces of V such that $W_1 \oplus W_2 = V$. Then,

$$B = B|_{W_1} \oplus B|_{W_2},$$

if

$$B(w_1, w_2) = 0, \text{ for all } w_1 \in W_1 \text{ and } w_2 \in W_2.$$

Hence, this direct sum is often called orthogonal sum. Next, we are going to define the concept of radical.

Definition 56 (Radical)**.** Let $B : V \times V \to F$ be a bilinear form. Define

$$\text{rad}_L(V) = \{v \in V : B(v, w) = 0, \text{ for all } w \in V\}$$
$$\text{rad}_R(V) = \{v \in V : B(w, v) = 0, \text{ for all } w \in V\}$$

Definition 57 (Non-degenerate)**.** A bilinear form is non-degenerate if $\text{rad}_R(V) = \{0\}$.

In fact, the following three statements are equivalent:

1. $\text{rad}_R(V) = \{0\}$.
2. $\text{rad}_L(V) = \{0\}$.
3. $\det \Omega_B \neq 0$.

Definition 58 (Alternating and symmetric bilinear forms)**.** Let $B : V \times V \to F$ be a bilinear form.

1. B is alternating if $B(v, w) = -B(w, v)$, for all $v, w \in V$.
2. B is symmetric if $B(v, w) = B(w, v)$, for all $v, w \in V$.

We first discuss the alternating form. Now, suppose B is non-degenerate and alternating. Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be a basis of V and let $\Omega_B = \left(B(v_i, v_j)\right)$ be the matrix attached to $\mathcal{A}$. Then,

$$\Omega_B{}^{\text{t}} = -\Omega_B.$$

If a matrix $A \in M_n(F)$ satisfied $A^{\text{t}} = -A$, then it is called skew-symmetric. Next, we want to find a basis $\mathcal{A}$ such that the matrix $\Omega_{B,\mathcal{A}}$ is as simple as possible.

Definition 59 (Symplectic basis)**.** A basis $\{e_1, e_2, \dots, e_r, f_1, f_2, \dots, f_r\}$ ($\dim V = 2r$) of V is called a symplectic basis for B if

1. $B(e_i, e_j) = B(f_i, f_j) = 0$, for all i, j.
2. $B(e_i, f_j) = 0$, if $i \neq j$.
3. $B(e_i, f_i) = 0$, for all i.

In other words, if $\mathcal{A}$ is a symplectic basis, then

$$\Omega_{B,\mathcal{A}} = \begin{pmatrix} O_r & I_r \\ -I_r & O_r \end{pmatrix},$$

where $O_r, I_r \in M_r(F)$ are the zero matrix and the identity matrix, respectively.

Theorem 60. *Assume* $\mathrm{char}(F) \neq 2$. *If V is equipped with a non-degenerate and alternating form B, then* $\dim V$ *is even and V has a symplectic basis.*

Proof. B is alternating and $\mathrm{char}(F) \neq 2$, so for any $v \in V$,

$$B(v,v) = -B(v,v) \implies B(v,v) = 0.$$

Let $e_1 \in V \setminus \{0\}$. Choose f_1 such that $B(e_1, f_1) = 1$. (This could be done because B is non-degenerate.) Let $W = Fe_1 \oplus Ff_1 = \mathrm{span}_F\{e_1, f_1\}$. We define $W^\perp$ as

$$W^\perp := \{v \in V : B(v,w) = 0, \text{ for all } w \in W\}.$$

We claim $V = W \oplus W^\perp$ is an internal direct sum as vector space with bilinear form. To see this, it suffices to show that $V = W \oplus W^\perp$ is an internal direct sum as vector space. ($\because B(W, W^\perp) = 0$.)

1. W and $W^\perp$ is linearly independent.
   It is equivalent to prove $W \cap W^\perp = \{0\}$. Let $v \in W \cap W^\perp$. Then, $v = a \cdot e_1 + b \cdot f_1$ for some $a, b \in F$.

   $$v \in W^\perp \implies B(v, e_1) = a = 0; \quad B(v, e_2) = b = 0.$$

2. W and $W^\perp$ generate V.
   It is equivalent to prove for each $v \in V$, there exist $a, b \in F$ such that

   $$(v - a \cdot e_1 - b \cdot f_1) \in W^\perp.$$

   Some simple calculations show that

   $$a = B(v, f_1), \quad b = -B(v, e_1),$$

   satisfies the condition.

Thus, $(V, B) = (W, B|_W) \oplus (W^\perp, B|_{W^\perp})$. Note that $B|_{W^\perp}$ is a non-degenerate (why?) and alternating form. By induction, $\dim W^\perp = 2r - 2$ for some $r \in \mathbb{N}$, and $W^\perp$ has a symplectic basis $\{e_2, e_3, \dots, e_r, f_2, f_3, \dots, f_r\}$ for $B|_{W^\perp}$. We conclude that $\dim V = 2r$ and $\{e_1, e_2, \dots, e_r, f_1, f_2, \dots, f_r\}$ is a symplectic basis for (V, B). □

Now, we discuss the non-degenerate symmetric form on V.

Theorem 61. *Assume* $\mathrm{char}(F) \neq 2$. *If V is equipped with a non-degenerate and symmetric form B, then there exist a basis $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ of V such that*

$$B(v_i, v_j), \text{ if } i \neq j.$$

In other words,

$$\Omega_{B,\mathcal{A}} = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$$

is a diagonal matrix where $a_i = B(v_i, v_i)$. Note that $a_i \neq 0$ since B is non-degenerate.

Proof. We claim that there exists $v \in V \setminus \{0\}$ such that $B(v, v) \neq 0$. If such v does not exist, then

$$2B(v, w) = B(v + w, v + w) - B(v, v) - B(w, w) = 0, \text{ for all } v, w \in V.$$

Since $\text{char}(F) \neq 2$, we have $B(v, w) = 0$ for all $v, w \in V$. Therefore, there exists $v_1 \in V \setminus \{0\}$ such that $B(v_1, v_1) \neq 0$. Let $W = Fv_1$ and let

$$W^{\perp} := \{v \in V : B(v, v_1) = 0\}.$$

Then, $(V, B) = (W, B|_W) \oplus (W^{\perp}, B|_{W^{\perp}})$ and we can proceed by induction. □

Next, we can classify all symmetric bilinear forms on finite dimensional vector space over $\mathbb{R}$. Let V be a real vector space with a symmetric bilinear form B. Suppose B is non-degenerate, then by Theorem 61, there is a basis $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ such that

$$\Omega_{B,\mathcal{A}} = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \quad (a_i \neq 0.)$$

Replacing $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ with $\mathcal{A}'$

$$\left\{ \frac{v_1}{\sqrt{|a_1|}}, \frac{v_2}{\sqrt{|a_2|}}, \dots, \frac{v_n}{\sqrt{|a_n|}} \right\},$$

then

$$\Omega_{B,\mathcal{A}'} = \begin{pmatrix} \text{sgn}(a_1) & & & \\ & \text{sgn}(a_2) & & \\ & & \ddots & \\ & & & \text{sgn}(a_n) \end{pmatrix}.$$

Thus, we can define the signature of a non-degenerate symmetric bilinear form by counting the positive and negative elements on the diagonal matrix $\Omega_{B,\mathcal{A}}$.

Definition 62 (Signature)**.** If B is a non-degenerate symmetric bilinear form on a vector space V over $\mathbb{R}$, then define the signature (r, s) of V so that

1. $r = \#\{i : \text{sgn}(a_i) = 1\}$.
2. $s = \#\{i : \text{sgn}(a_i) = -1\}$.

We have $r + s = \dim V$ since B is non-degenerate.

If B is degenerate (and symmetric), we also can define its signature. Note that $\mathrm{rad}_L(V) = \mathrm{rad}_R(V)$ (B is symmetric.) Then, $V/\mathrm{rad}(V)$ is a vector space, and induced a bilinear form $\tilde{B}$ from B defined by

$$\tilde{B}([v_1],[v_2]) = B(v_1, v_2).$$

It is easy to see that $\tilde{B}$ is well-defined and one can check that $\tilde{B}$ is a non-degenerate symmetric bilinear form. We define the signature of B to be the signature of $\tilde{B}$.

Theorem 63 (Sylvester's Law of Inertia)**.** *Non-degenerate symmetric bilinear forms over finite dimensional real vector spaces are completely determined by their signature. That is, there exists a bijection preserving the bilinear form structure if two spaces have the same signature. In other words, signature is a well-defined invariant for V up to isometries.*

Remark.

1. Theorem 63 is a corollary of Theorem 72, we will not give the proof here.
2. The non-degenerate symmetric bilinear form B is positive definite (inner product) if the signature of B is $(\dim V, 0)$.

2.8 Quadratic forms and Witt decomposition

In this subsection, we assume F is one of the fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_p$ ($p \neq 2$). Let V be a finite dimensional vector space over F.

Definition 64. A quadratic form $Q : V \to F$ is a function on V such that

1. $Q(\alpha v) = \alpha^2 Q(v)$.
2. The map $B_Q : V \times V \to F$ defined by

$$(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$$

is a bilinear form.

This bilinear form B_Q is called the bilinear form attached to Q.

In fact, we have a bijection between symmetric bilinear forms and quadratic forms. If B is a symmetric bilinear form, then

$$Q(x) = \frac{1}{2}B(x, x)$$

is a quadratic form. Similarly, if Q is a quadratic form, then B_Q define in the Definition 64 is a symmetric bilinear form. Moreover, if $\dim_F V = n$, then there is a bijection between all quadratic forms and all homogeneous polynomial $F[x_1, x_2, \dots, x_n]$ with degree 2.

Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be a basis of V, then

$$Q\left(\sum_{i=1}^{n} \alpha_i v_i\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \frac{1}{2}\alpha_i B_Q(v_i, v_j)\alpha_j \overset{\mathcal{A}}{\longleftrightarrow} \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}x_i x_j \in F[x_1, x_2, \dots, x_n].$$

The polynomial on the right side is called the polynomial attached to Q, and denote it by f_Q. Thus, we can study the property of quadratic forms and convert it to the language of polynomials or bilinear forms.

Definition 65. A quadratic space is a vector space V equipped with a quadratic form Q (or a symmetric bilinear form, because of the bijection we just demonstrated.)

Definition 66 (Isometric and isometry)**.** Let (V_1, Q_1) and (V_2, Q_2) be two quadratic spaces. We say V_1 and V_2 are isometric if V_1 is isomorphic to V_2 as a quadratic space. Namely, there exists a isomorphism $T : V_1 \to V_2$ as vector spaces such that

$$Q_2(T(v)) = Q_1(v), \text{ for all } v \in V_1.$$

Such isomorphism T is called an isometry.

The quadratic space is kind of like a generalization of inner product spaces. Here we show an example of isometry. Let (V, Q) be a quadratic space. Let $v_0 \in V$ with $Q(v_0) \neq 0$. Define

$$\begin{aligned} T : V &\to V \\ x &\mapsto x - \frac{2B_Q(x, v_0)}{B_Q(v_0, v_0)} v_0, \end{aligned}$$

where B_Q is the bilinear form associated with the quadratic form Q. We claim that T is an isometry. Note that

$$\begin{aligned} Q(T(x)) &= Q(x - \frac{2B_Q(x, v_0)}{B_Q(v_0, v_0)} v_0) \\ &= B_Q(x, -\frac{2B_Q(x, v_0)}{B_Q(v_0, v_0)} v_0) + Q(x) + \left(\frac{2B_Q(x, v_0)}{B_Q(v_0, v_0)}\right)^2 Q(v_0) \\ &= -\frac{2B_Q(x, v_0)}{B_Q(v_0, v_0)} B_Q(x, v_0) + Q(x) + \left(\frac{2B_Q(x, v_0)}{B_Q(v_0, v_0)}\right)^2 \cdot \frac{1}{2} B_Q(v_0, v_0) \\ &= Q(x) \end{aligned}$$

holds for all $x \in V$. T is like the reflection define in inner product spaces. We call T the reflection along the hyperplane orthogonal to v_0 with respect to the quadratic form Q. Also, we found that $Q(v_0)$ is an important property. so we give the following definitions.

Definition 67. Given a quadratic space (V, Q). Define the following terminologies.

1. V is non-degenerate if the bilinear form B_Q associated with Q is non-degenerate.
2. A vector $v \in V$ is isotropic if $Q(v) = 0$.
3. A vector $v \in V$ is anisotropic if $Q(v) \neq 0$.
4. A quadratic space is isotropic if V is non-degenerate and contains an isotropic vector.
5. A quadratic space is anisotropic if V every non-zero vector in V is anisotropic.

6. A subspace $W \subset V$ is totally isotropic if $Q|_W = 0$.

Definition 68 (Hyperbolic plane)**.** A 2-dimensional quadratic space $\mathbb{H}$ is called a hyperbolic plane if $f_Q(x_1, x_2) = x_1 x_2$ for a suitable choice of basis. (Recall that f_Q is the polynomial attached to Q.) In other words, there exists a basis $\{v_1, v_2\}$ such that

$$\big(B_Q(v_i, v_j)\big) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Theorem 69. *Let V be a non-degenerate quadratic space. Let $U \subset V$ be a totally isotropic subspace with a basis $\{u_1, u_2, \dots, u_m\}$. Then, there exists a totally isotropic subspace $U' = \operatorname{span}_F\{u_1', u_2', \dots, u_m'\}$ such that*

$$B(u_i, u_j') = \begin{cases} 1 & \text{, if } i = j \\ 0 & \text{, otherwise} \end{cases}.$$

Proof. We prove by induction on $\dim_F U = m$. If $m = 1$, $U = F \cdot u_1$. Since V is non-degenerate, B_Q is non-degenerate. Thus, there exists a vector $w \in V$ such that $B_Q(u_1, w) = 1$. Note that $w \notin F \cdot u_1$, otherwise $B_Q(u_1, w) = 0$. Let $u_1' = w + \alpha \cdot u_1$, we claim that there is an $\alpha \in F$ such that $Q(u_1') = 0$. (Undetermined coefficient method.) Then,

$$Q(u_1') = Q(w + \alpha \cdot u_1) = B_Q(w, \alpha \cdot u_1) + Q(w) + Q(u_1) = \alpha + Q(w).$$

Hence, $u_1' = w - Q(w)u_1$ satisfies the requirement.

Now, suppose the assertion is true for some $m = k \in \mathbb{N}$. Assume $m = k + 1 > 1$. Let $W = \operatorname{span}_F\{u_2, u_3, \dots, u_m\} \subset U \subset V$ be a totally isotropic subspace. Define $W^\perp := \{v \in V : B_Q(v, w) = 0, \text{ for all } w \in W\}$. Then, $F \cdot u_1 \subset W^\perp$ is an totally isotropic subspace. Note that $Q|_{W^\perp}$ is non-degenerate (otherwise Q would be degenerate). Thus, by the previous step, there exists $u_1' \in W^\perp$ such that $H_1 := \operatorname{span}_F\{u_1, u_1'\}$ is a hyperbolic plane and $B_Q(u_1, u_1') = 1$.

Since $H_1 \subset W^\perp$, we have $W \subset H_1^\perp$, $\dim W \leq k$, and $Q|_{H_1^\perp}$ is non-degenerate. By the induction hypothesis, there exists a totally isotropic subspace $\operatorname{span}_F\{u_2', u_3', \dots, u_m'\} \subset H_1^\perp$ such that

$$B_Q(u_i, u_j') = \begin{cases} 1 & \text{, if } i = j \\ 0 & \text{, otherwise} \end{cases} \qquad (2 \leq i, j \leq m).$$

Then, $U' = \operatorname{span}_F\{u_1', u_2', \dots, u_m'\}$ is the desired subspace. □

Corollary. Let V be a non-degenerate quadratic space and $U \subset V$ be a totally isotropic subspace with dimension m. Then, there exists a totally isotropic subspace U' such that

$$U \cap U' = \{0\}, \quad \text{and} \quad U \oplus U' \simeq \mathbb{H}^m.$$

Theorem 70 (Witt decomposition)**.** *Let V be a quadratic space. Then we have the following orthogonal direct sum,*

$$V \simeq \operatorname{rad}(V) \oplus \mathbb{H}^m \oplus V_0,$$

where $\operatorname{rad}(V)$ *is the radical of* (V, B_Q), $\mathbb{H}$ *denote a hyperbolic plane, and V_0 is an anisotropic quadratic space. Note that $\simeq$ means isometric.* (*Recall Definition 66.*)

Proof. Choose any subspace $W \subset V$ such that $V = \operatorname{rad}(V) \oplus W$ (as vector spaces). Then, $\operatorname{rad}(V) \perp W$ by the definition of the radical of V. This indicate that $V = \operatorname{rad}(V) \oplus W$ as quadratic spaces. (Recall the direct sum of vector spaces with bilinear form.) Also, $(W, Q|_W)$ is non-degenerate. (why?) Thus, we may assume V is non-degenerate, that is $\operatorname{rad}(V) = \{0\}$. We prove by induction on $\dim V$. If $\dim V = 1$, then V is anisotropic.

Now, suppose $\dim V > 1$ and V is NOT anisotropic. Then, there exists $u \in V \setminus \{0\}$ such that u is isotropic, namely, $Q(u) = 0$. From Theorem 69, we obtain that there is $u' \in V$ such that

$$B_Q(u, u') = 1 \quad \text{and} \quad u \text{ is isotropic.}$$

Hence, $H := \operatorname{span}_F\{u, u'\}$ is a hyperbolic plane. We can decompose V into $V = H \oplus H^\perp$. Then, we have $Q|_{H^\perp}$ is non-degenerate and $\dim H^\perp < \dim V$, so we can apply the induction hypothesis on $H^\perp$. Therefore, $H^\perp \simeq \mathbb{H}^{m-1} \oplus V_0$, where V_0 is an anisotropic subspace. This completes the proof. □

Next, we are going to prove that such orthogonal direct sum is unique. We first prove the following theorem.

Theorem 71 (Witt cancellation Theorem)**.** *Let V_1, V_2, U_1, and U_2 be finite dimensional quadratic spaces over F. If $V_1 \simeq V_2$ and $V_1 \oplus U_1 \simeq V_2 \oplus U_2$ are two isometric relation. Then, $U_1 \simeq U_2$ is isometric.*

Proof. We first note that $V_2 \oplus U_2 \simeq V_1 \oplus U_1 \simeq V_2 \oplus U_1$, thus we may assume $V_1 = V_2 = V$.

Case 1: V is totally isotropic and U_1 is non-degenerate.

Write T to denote the isometry of $V \oplus U_1$ to $V \oplus U_2$. Let $\mathcal{A} = \{v_1, \dots, v_n\}$, $\mathcal{B}_1 = \{u_1, \dots, u_r\}$, and $\mathcal{B}_2 = \{w_1, \dots, w_r\}$ be bases of V, U_1, and U_2 respectively. Let the matrices of quadratic form on $V \oplus U_2$ with respect to $T(\mathcal{A}) \sqcup T(\mathcal{B}_1)$ and $\mathcal{A} \sqcup \mathcal{B}_2$ be

$$M_1 = \begin{pmatrix} 0 & 0 \\ 0 & B_1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 0 \\ 0 & B_2 \end{pmatrix} \qquad \text{respectively.}$$

Here B_i is the matrix of the quadratic form of U_i. (It is useful here that V is totally isotropic and the the direct sum is "orthogonal" direct sum.) Since $V \oplus U_1 \simeq V \oplus U_2$, there is an invertible matrix $P \in M_{n+r}(F)$ such that

$$P^{\mathrm{t}} \cdot M_2 \cdot P = M_1.$$

If we write

$$P = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where $A \in M_n(F)$ and $D \in M_r(F)$, then we have $D^{\mathrm{t}} \cdot B_2 \cdot D = B_1$. Note that we assume U_1, or more precisely, the bilinear form that U_1 equipped with, is non-degenerate, thus B_1 is invertible and so is D. This shows that U_1 and U_2 are isometric.

Case 2: V is totally isotropic.

Write $U_1 = \operatorname{rad}(U_1) \oplus W_1$ and $U_2 = \operatorname{rad}(U_2) \oplus W_2$, where W_1 and W_2 are non-degenerate quadratic space. Then,

$$\begin{aligned} V \oplus U_1 \simeq V \oplus U_2 &\implies V \oplus \operatorname{rad}(U_1) \oplus W_1 \simeq V \oplus \operatorname{rad}(U_2) \oplus W_2 \\ &\implies \operatorname{rad}(V \oplus U_1) = V \oplus \operatorname{rad}(U_1) \simeq V \oplus \operatorname{rad}(U_2) = \operatorname{rad}(V \oplus U_2) \end{aligned}$$

By Case 1, $W_1 \simeq W_2$. It is obvious that $\operatorname{rad}(V_1) \simeq \operatorname{rad}(V_2)$. Thus we have $U_1 \simeq U_2$.

Case 3: For general V.

We prove by induction on $n = \dim V$. If $n = 1$, write $V = F \cdot v$. If v is isotropic, then the Theorem follows from Case 2. Now, suppose v is anisotropic. Let T denote the isometry of $Fv \oplus U_1$ to $Fv \oplus U_2$. We have

$$F(T(v)) \oplus T(U_1) \simeq Fv \oplus U_2.$$

By Lemma 9, there is an isometry $\tau : Fv \oplus U_2 \to Fv \oplus U_2$ such that

$$\tau(T(v)) = v.$$

It follows that

$$\tau \circ T(U_1) = (Fv)^{\perp} = U_2.$$

Therefore, $\tau \circ T$ is an isometry of U_1 to U_2. Now, suppose $n = \dim V > 1$, then $V = Fv_1 \oplus Fv_2 \oplus \cdots \oplus Fv_n$ (orthogonal direct sum) with $Q(v_i) = a_i$ $(1 \le i \le n)$. This is possible because of Theorem 61. It follows that

$$\begin{aligned} V \oplus U_1 \simeq V \oplus U_2 &\implies Fv_1 \oplus (Fv_2 \oplus \cdots \oplus Fv_n \oplus U_1) \simeq Fv_1 \oplus (Fv_2 \oplus \cdots \oplus Fv_n \oplus U_2) \\ &\implies Fv_2 \oplus \cdots \oplus Fv_n \oplus U_1 \simeq Fv_2 \oplus \cdots \oplus Fv_n \oplus U_2 \\ &\implies U_1 \simeq U_2 \qquad \text{(by the induction hypothesis)}. \end{aligned}$$

The discussions above prove the theorem. □

Lemma 9. If $x, y \in V$ are two anisotropic vectors in a quadratic space, such that $Q(x) = Q(y)$. Then there exists an isometry $\tau : V \to V$ with $\tau(x) = y$.

Proof.

Case 1: $x - y$ is anisotropic.

Consider $\tau = T_{x-y}$ the reflection along the hyperplane orthogonal to the vector $x - y$. Precisely, we define

$$\tau(v) = v - 2 \cdot \frac{B_Q(v, x-y)}{B_Q(x-y, x-y)} \cdot (x-y).$$

Plug in $v = x$ gives

$$\begin{aligned} \tau(x) &= x - 2 \cdot \frac{B_Q(x, x-y)}{B_Q(x-y, x-y)} \cdot (x-y) \\ &= x - 2 \cdot \frac{B_Q(x,x) - B_Q(x,y)}{2 \cdot \big(B_Q(x,x) - B_Q(x,y)\big)} \cdot (x-y) \qquad (\because Q(x) = Q(y)) \\ &= x - (x-y) = y. \end{aligned}$$

Case 2: $x - y$ is isotropic.

Note that $Q(x-y) + Q(x+y) = 2\left(Q(x) + Q(y)\right)$ (By Parallelogram Theorem.) This shows that $-x - y$ is isotropic if $x - y$ is anisotropic. Let $\tau = T_{-x-y} \circ -\mathrm{Id}_V$ be a composition of two isometries. Then $\tau(x) = T_{-x-y}(-x) = y$.

The discussions above complete the proof. □

Now, we can prove the following theorem.

Theorem 72 (Uniqueness of Witt Decomposition)**.** *Let V be a quadratic space. If*

$$V \simeq \mathrm{rad}\,(V) \oplus \mathbb{H}^m \oplus V_0 \simeq \mathrm{rad}\,(V) \oplus \mathbb{H}^{m'} \oplus V_0',$$

where V_0 and V_0' are anisotropic, then $m = m'$ and $V_0 \simeq V_0'$.

Proof. Witt Cancellation Theorem (Theorem 71) shows that

$$\mathbb{H}^m \oplus V_0 \simeq \mathbb{H}^{m'} \oplus V_0'.$$

We claim that m is the dimensional of maximal totally isotropic subspaces of $\mathbb{H}^m \oplus V_0$, this can be seen from the proof of Theorem 70. Thus, $m = m'$ and it follows from Witt Cancellation Theorem (Theorem 71) that $V_0 \simeq V_0'$. □

Recall that in the last subsection, we introduced the concept of signature. There is a theorem we have not proved yet. Here we have a fast way to prove it. *Proof of Theorem 63.* If (V, B) has signature (p, q). Without much loss of generality, we assume $p \geq q$. Then, $V \simeq \mathbb{H}^q \oplus I_{p-q}$, where $I_{p-q} = \mathbb{R} \cdot v_1 \oplus \cdots \oplus \mathbb{R} \cdot v_{p-q}$ is an anisotropic space such that

$$Q(\sum_{i=1}^{p-q} x_i v_i) = \sum_{i=1}^{p-q} x_i^2.$$

This shows there is a 1-1 correspondence between signatures and Witt decompositions. This proves the theorem. □

Theorem 73 (Cartan-Dieudonné Theorem)**.** *Let V be a non-degenerate quadratic space with dimension n. Let the orthogonal group of V be $\mathrm{O}(V) = \{T : V \to V,\ T \text{ is isometry}\}$. Then for each $\sigma \in O(V)$, σ is a product of at most n reflections.*

In fact we have proved this theorem, when V is an inner product space over $\mathbb{R}$, then we can use the spectral theory of inner product space. However, we do not have these tools here, hence the proof is much harder.

Proof. We first write $\mathrm{O}(V) = \Sigma_1 \sqcup \Sigma_2 \sqcup \Sigma_3$, where

$$\Sigma_1 = \{\sigma \in \mathrm{O}(V) : \exists \text{ anisotropic } x \in V \text{ such that } \sigma(x) = x\}$$
$$\Sigma_2 = \{\sigma \in \mathrm{O}(V) : \exists \text{ anisotropic } x \in V \text{ such that } \sigma(x) - x \neq 0 \text{ and is anisotropic}\}$$
$$\Sigma_3 = \{\sigma \in \mathrm{O}(V) : \forall \text{ anisotropic } x \in V,\ \sigma(x) - x \neq 0 \text{ and is isotropic}\}$$

We will prove by induction on $n = \dim V$. If $n = 1$ then $\mathrm{O}(V) = \{\pm 1\}$. Now suppose $n > 1$. Let $\sigma \in \mathrm{O}(V)$.

Case 1: If $\sigma \in \Sigma_1$, then there exists an anisotropic vector $x \in V$ such that $\sigma(x) = x$. Write $V = Fx \oplus (Fx)^\perp$ as orthogonal sum of σ-invariant subspace. By induction, $\sigma|_{(Fx)^\perp} = \tau_1 \cdots \tau_r$ for some reflections τ_i where $r \leq n-1$. Define the extension $\widetilde{\tau_i}$ of τ_i to V by $\widetilde{\tau_i}(x) = x$ and $\widetilde{\tau_i}(y) = \tau_i(y)$ for $y \in (Fx)^\perp$. Then $\widetilde{\tau_i}$ is a reflection in V and

$$\sigma = \widetilde{\tau_1} \cdots \widetilde{\tau_r}.$$

Case 2: If $\sigma \in \Sigma_2$, then there exists an anisotropic vector $x \in V$ such that $v = \sigma(x) - x$ is non-zero and anisotropic. Then $T_v(\sigma(x)) = x$, T_v is the reflection along the hyperplane perpendicular to the vector v. Case 1 gives $T_v \cdot \sigma = \tau_1 \cdots \tau_r$, where r is at most $n-1$. Thus,

$$\sigma = T_v \cdot \tau_1 \cdots \tau_r$$

is a product of at most n reflections.

Case 3: Suppose $\sigma \in \Sigma_3$. We first claim that $n \geq 3$ and for all $x \in V$, $\sigma(x) - x$ is isotropic. The first assertion could be checked by considering the matrix attached to the quadratic form Q. To see the second assertion, we suppose $x \in V$ is an isotropic vector and let $y \in V$ be an anisotropic vector such that $B(x, y) = 0$ (the existence of y is trivial). Now for all $a \in F$ we have $Q(x + ay) \neq 0$ hence we obtain

$$Q(\sigma(x + ay) - (x + ay)) = 0, \qquad Q(\sigma(y) - y) = 0.$$

It follows that

$$Q(\sigma(x) - x) + 2a \cdot B(\sigma(y) - y, \sigma(z) - z) = 0, \text{ for all } a \in F.$$

Plugging in $a = \pm 1$ gives the desired result. Now, put $W := \mathrm{Im}(1 - \sigma) = (\mathrm{Id}_V - \sigma)V$. Then the result above implies that $Q|_W \equiv 0 \implies W \subset W^\perp$.

We now claim that $Q|_{W^\perp}$ and therefore $W^\perp \subset W^{\perp\perp} = W$. If $x \in W$ and $y \in W^\perp$ then we have

$$\begin{aligned} B(x, \sigma(y) - y) &= B(\sigma(x), \sigma(y) - y) - B(\sigma(x) - x, \sigma(y) - y) = B(\sigma(x), \sigma(y) - y) \\ &= B(\sigma(x), \sigma(y)) - B(\sigma(x), y) = B(x, y) - B(\sigma(x), y) \\ &= -B(x - \sigma(x), \sigma(y)) = 0. \end{aligned}$$

The nondegeneracy of B shows that $\sigma(y) = y$ for all $y \in W^\perp$. By assumption, y must be isotropic, that is $Q(y) = 0 \implies Q|_{W^\perp} \equiv 0$. Hence, we now have $W = W^\perp$. From Theorem 69 we know that there is a totally isotropic subspace $W' \subset V$ such that $W \cap W' = \{0\}$ and that

$$W \oplus W' \simeq \mathbb{H}^m,$$

for $m = \dim W$. Note that $V = W \oplus W'$ since $W = W^\perp$. Moreover, we have $\sigma|_W = \mathrm{Id}_W$.

We now finally claim that $\det \sigma = 1$. We observe that: for $x \in W$ and $y \in W'$, we have

$$B(x, \sigma(y) - y) = B(x, \sigma(y)) - B(x, y) = B(x, \sigma(y)) - B(\sigma(x), \sigma(y)) = 0.$$

Thus we conclude that $\sigma(y) - y \in W$. Let $\mathcal{B} = \{w_1, \ldots, w_m\}$ and $\mathcal{B}' = \{w'_1, \ldots, w'_m\}$ be bases of W and W', respectively.

Then,

$$[\sigma]_{\mathcal{B}\sqcup\mathcal{B}'} = \begin{pmatrix} I_m & * \\ 0 & I_m \end{pmatrix}.$$

This shows that $\det\sigma = 1$. Let τ be any reflection. Then $\tau\cdot\sigma \in \Sigma_1 \sqcup \Sigma_2$, since $\det\tau = -1$ for any reflection τ. Thus, $\tau\cdot\sigma$ is a product of at most n reflections. Thus, we conclude that σ is a product of at most $n+1$ reflections. However, note that $\det\sigma = 1$ and $\det\tau = -1$ for every reflection τ, hence σ is not a product of $n+1 = 2m+1$ reflections. This completes the proof.

□

Remark. In the 2016 video, due to the limited time, only the general steps of the proof are sketched, and the complete proof is not given. Here, I also refer to this article [1] for the proof.

3 Applications of Linear Algebra

In this section, we will introduce some applications of linear algebra.

3.1 The number of common zeros of two polynomials

First, we look at the following question. Let $f(x), g(x)$ be two polynomials.

What is the size of $\#\{a \in \mathbb{C} : f(a) = g(a) = 0\}$. (*Counted with multiplicities*)

The solution to this question is answered by Étienne Bézout, a French mathematician. Actually, I am not pretty sure whether the result is discovered by him, but to prove the result, we have to introduce a matrix called Bézoutian. We first define $v(f,g)$ to simplify our notation.

Definition 74. Let $f, g \in \mathbb{C}[x]$. Define

$$\begin{aligned} v(f,g) &= \text{the common roots of } f(x) \text{ and } g(x) \text{ counted with multiplicities} \\ &= \deg\left(\gcd\left(f(x), g(x)\right)\right). \end{aligned}$$

Definition 75 (Bézoutian or Bézout matrix)**.** Let $f, g \in \mathbb{C}[x]$ be two polynomials and let $n = \max\{\deg f, \deg g\}$. Then the Bézoutian $B_{f,g} = (b_{ij}) \in M_n(\mathbb{C})$ is a matrix such that

$$\frac{f(x)g(y) - f(y)g(x)}{x-y} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} x^i \cdot b_{ij} \cdot y^j = \begin{pmatrix} 1 & x & \cdots & x^{n-1} \end{pmatrix} \cdot B_{f,g} \cdot \begin{pmatrix} 1 \\ y \\ \vdots \\ y^{n-1} \end{pmatrix}.$$

If we define

$$V_n(x) = \begin{pmatrix} 1 & x & \cdots & x^{n-1} \end{pmatrix}^{\mathrm{t}},$$

then we have

$$\frac{f(x)g(y) - f(y)g(x)}{x-y} = V_n(x)^{\mathrm{t}} \cdot B_{f,g} \cdot V_n(y).$$

Theorem 76. *Let $f, g \in \mathbb{C}[x]$. We have*

$$v(f,g) = \text{nullity}(B_{f,g}).$$

Before proving this theorem, we shall introduce some notations, some lemmas and an important theorem.

Definition 77. Given

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x] \text{ and } g(x) = \sum_{i=0}^{n} b_i x^i \in \mathbb{C}[x].$$

Define the following matrices associated with $f(x)$ (and possibly $g(x)$).

1. The Hankel matrix of $f(x)$.
We usually write $H_f = (h_{ij}) \in M_n(\mathbb{C})$ to denote it. The entries are defined by:

$$h_{ij} = \begin{cases} a_{i+j-1} & \text{, if } i+j-1 < n \\ 0 & \text{, otherwise} \end{cases}.$$

That is,

$$H_f = \begin{pmatrix} a_1 & a_2 & \cdots & \cdots & a_n \\ a_2 & \ddots & \ddots & a_n & \\ \vdots & \ddots & a_n & & \\ \vdots & a_n & & & \\ a_n & & & & \end{pmatrix} \in M_n(\mathbb{C}).$$

2. The Toeplitz matrix of $f(x)$.
We usually write $T_f = (t_{ij}) \in M_n(\mathbb{C})$ to denote it. The entries are defined by:

$$t_{ij} = \begin{cases} a_{j-i} & \text{, if } i \le j \\ 0 & \text{, otherwise} \end{cases}.$$

That is

$$T_f = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ & a_0 & a_1 & \cdots & a_{n-2} \\ & & \ddots & \ddots & \vdots \\ & & & a_0 & a_1 \\ & & & & a_0 \end{pmatrix} \in M_n \in \mathbb{C}.$$

3. The anti-diagonal matrix.
We usually write $Z_n = (z_{ij}) \in M_n(\mathbb{C})$ to denote it. The entries are defined by

$$z_{ij} = \begin{cases} 1 & \text{, if } i+j = n+1 \\ 0 & \text{, otherwise} \end{cases}.$$

That is,

$$Z_n = \begin{pmatrix} & & & 1 \\ & & \iddots & \\ & \iddots & & \\ 1 & & & \end{pmatrix} \in M_n\mathbb{C}.$$

4. The resultant of f and g.
Let $n = \max\{\deg f, \deg g\}$. We write $R_{f,g} = (r_{ij}) \in M_{2n}(\mathbb{C})$ to denote the resultant. The entries are defined by

$$r_{ij} = \begin{cases} a_{j-i} & \text{, if } i \le n \text{ and } 0 \le j-i \le n \\ b_{j-i} & \text{, if } i > n \text{ and } 0 \le j-i \le n \\ 0 & \text{, otherwise} \end{cases}.$$

That is,

$$R_{f,g} := \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & & & \\ & a_0 & a_1 & \cdots & a_{n-1} & a_n & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & \cdots & a_{n-1} & a_n \\ b_0 & b_1 & \cdots & b_{n-1} & b_n & & & \\ & b_0 & b_1 & \cdots & b_{n-1} & b_n & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & b_0 & b_1 & \cdots & b_{n-1} & b_n \end{pmatrix} \in M_{2n}(\mathbb{C}).$$

Remark. In all the above matrices, all "blank" entries represent 0.

From the above definitions, it is easy to see

$$Z \cdot H_f = \begin{pmatrix} a_n & & & \\ a_{n-1} & a_n & & \\ \vdots & \ddots & \ddots & \\ a_1 & \cdots & a_{n-1} & a_n \end{pmatrix}; \quad Z \cdot T_f = \begin{pmatrix} & & & a_0 \\ & & a_0 & a_1 \\ & \iddots & \iddots & \vdots \\ a_0 & a_1 & \cdots & a_{n-1} \end{pmatrix}.$$

Thus, we have

$$R_{f,g} = \left(\begin{array}{c|c} T_f & Z \cdot H_f \\ \hline T_g & Z \cdot H_g \cdot \end{array}\right).$$

Theorem 78. *Let $f, g \in \mathbb{C}[x]$. We have*

$$v(f,g) = \text{nullity}(R_{f,g}).$$

Proof. Let $n := \max\{\deg f, \deg g\}$ and let P_k be the set of all complex polynomials with degree less than k. In other words,

$$P_k := \{p \in \mathbb{C}[x] : \deg p < k\}.$$

Consider a linear transformation T defined by:

$$\begin{aligned} T : P_n \oplus P_n &\to P_{2n} \\ (u, v) &\mapsto u \cdot f + v \cdot g \end{aligned}.$$

Suppose $d(x) = \gcd\Big(f(x), g(x)\Big)$, and we assume that $f(x) = h(x) \cdot d(x)$, $g(x) = k(x) \cdot d(x)$, and that $\gcd(h(x), k(x)) = 1$. Then,

$$\begin{aligned} \ker T &= \{(u, v) \in P_n \times P_n : u \cdot f + v \cdot g = 0\} \\ &= \{(u, v) \in P_n \times P_n : u \cdot h + v \cdot k = 0\} \\ &= \{(k \cdot \alpha, -h \cdot \alpha) : \alpha \in \mathbb{C}[x]\} \ (\because \gcd(k, h) = 1.) \end{aligned}$$

However, note the degree of α is less than $\deg d(x)$. This indicates that

$$\dim \ker T = \deg d(x) = v(f, g).$$

It suffices to show that $\dim \ker T = \text{nullity}(R_{f,g})$. It follows from the fact that

$$[T]_{\mathcal{B},\mathcal{A}} = {R_{f,g}}^{\mathsf{t}},$$

where $\mathcal{B}$ is the standard basis of $P_n \oplus P_n$ and $\mathcal{A}$ is the standard basis of P_{2n}. □

To prove Theorem 76, it remains to find the relation between $R_{f,g}$ and $B_{f,g}$.

Lemma 10. Let $f, g \in \mathbb{C}[x]$ and let $n = \max\{\deg f, \deg g\}$. H_f, T_f and Z are defined as above.

1. T_f and T_g commute, namely, $T_f \cdot T_g = T_g \cdot T_f$.
2. $X^{\mathsf{t}} = Z \cdot X \cdot Z$, for all $X \in M_n(\mathbb{C})$.
3. $H_f \cdot Z \cdot H_g = H_g \cdot Z \cdot H_f$.

The proof is omitted since it can be done by some simple calculations.

Lemma 11. Let $f, g \in \mathbb{C}[x]$. Then, $B_{f,g} = H_f \cdot T_g - H_g \cdot T_f$.

Proof. We write $R = R_{f,g}$ and $B = B_{f,g}$. It is easy to see that

$$\frac{x^n - y^n}{x - y} = V_n(x)^{\mathsf{t}} \cdot Z \cdot V_n(y).$$

Thus, we have

$$\begin{aligned} &(x^n - y^n) \cdot \frac{f(x)g(y) - f(y)g(x)}{x - y} \\ =& V_n(x)^{\mathsf{t}} \cdot \Big(Z \cdot \Big(f(x)g(y) - f(y)g(x)\Big)\Big) \cdot V_n(y) \\ =& \begin{pmatrix} V_n(x) \cdot f(x) \\ V_n(x) \cdot g(x) \end{pmatrix}^{\mathsf{t}} \cdot \begin{pmatrix} 0 & Z \\ -Z & 0 \end{pmatrix} \cdot \begin{pmatrix} f(y) \cdot V_n(y) \\ g(y) \cdot V_n(y) \end{pmatrix} \\ =& V_{2n}(x)^{\mathsf{t}} \cdot R^{\mathsf{t}} \cdot \begin{pmatrix} 0 & Z \\ -Z & 0 \end{pmatrix} \cdot R \cdot V_{2n}(y) \text{ (by direct computation.)} \end{aligned}$$

On the other hand, we have the left hand side is equal to

$$\begin{aligned}
&(x^n - y^n) \cdot V_n(x)^{\mathrm{t}} \cdot B_{f,g} \cdot V_n(y) \\
&= V_n(x)^{\mathrm{t}} \cdot \left(x^n \cdot B_{f,g}\right) \cdot V_n(y) - V_n(x)^{\mathrm{t}} \cdot \left(B_{f,g} \cdot y^n\right) \cdot V_n(y) \\
&= V_{2n}(x)^{\mathrm{t}} \cdot \begin{pmatrix} 0 & 0 \\ B & 0 \end{pmatrix} \cdot V_{2n}(y) - V_{2n}(x)^{\mathrm{t}} \cdot \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \cdot V_{2n}(y) \\
&= V_{2n}(x)^{\mathrm{t}} \cdot \begin{pmatrix} 0 & -B \\ B & 0 \end{pmatrix} \cdot V_{2n}(y).
\end{aligned}$$

Therefore, we conclude that

$$\begin{aligned}
&\begin{pmatrix} 0 & -B \\ B & 0 \end{pmatrix} = R^{\mathrm{t}} \cdot \begin{pmatrix} 0 & Z \\ -Z & 0 \end{pmatrix} \cdot R \\
\implies &\begin{pmatrix} 0 & -B \\ B & 0 \end{pmatrix} = \begin{pmatrix} T_f^{\mathrm{t}} & T_g^{\mathrm{t}} \\ H_f^{\mathrm{t}} \cdot Z & H_g^{\mathrm{t}} \cdot Z \end{pmatrix} \cdot \begin{pmatrix} 0 & Z \\ -Z & 0 \end{pmatrix} \cdot \begin{pmatrix} T_f & Z \cdot H_f \\ T_g & Z \cdot H_g \end{pmatrix} \\
\implies &\begin{pmatrix} 0 & -B \\ B & 0 \end{pmatrix} = \begin{pmatrix} Z \cdot T_f \cdot Z & Z \cdot T_g \cdot Z \\ H_f \cdot Z & H_g \cdot Z \end{pmatrix} \cdot \begin{pmatrix} Z \cdot T_g & H_g \\ -Z \cdot T_f & -H_f \end{pmatrix} \\
\implies &\begin{pmatrix} 0 & -B \\ B & 0 \end{pmatrix} = \begin{pmatrix} 0 & * \\ X & 0 \end{pmatrix}, \text{ where } X = H_f \cdot T_g - H_g \cdot T_f \\
\implies &B = X = H_f \cdot T_g - H_g \cdot T_f.
\end{aligned}$$

The above deductions have used Lemma 10. □

Now, we can start proving Theorem 76.

Proof of Theorem 76. It suffices to show that nullity$(R_{f,g})$ = nullity$(B_{f,g})$. Without loss of generality, we assume that $\deg f \geq \deg g$. Hence, $a_n \neq 0$ if $n = \max\{\deg f, \deg g\}$. Consider

$$\begin{aligned}
\begin{pmatrix} I_n & O_n \\ T_f & ZH_f \end{pmatrix} \cdot R &= \begin{pmatrix} I_n & O_n \\ T_f & ZH_f \end{pmatrix} \cdot \begin{pmatrix} T_f & ZH_f \\ T_g & ZH_g \end{pmatrix} \\
&= \begin{pmatrix} T_f & ZH_f \\ T_f^2 + ZH_fT_g & T_fZH_f + ZH_fZH_g \end{pmatrix} \\
&= \begin{pmatrix} T_f & ZH_f \\ ZB + (ZH_g + T_f)T_f & (T_f + ZH_g)ZH_f \end{pmatrix} \\
&\qquad \text{(Recall that } B = H_fT_g - H_gT_f \text{ and Lemma 10)} \\
&= \begin{pmatrix} O_n & I_n \\ ZB & T_f + ZH_g \end{pmatrix} \cdot \begin{pmatrix} I_n & O_n \\ T_f & ZH_f \end{pmatrix} \\
&= \begin{pmatrix} O_n & I_n \\ Z & T_f + ZH_g \end{pmatrix} \cdot \begin{pmatrix} B & O_n \\ O_n & I_n \end{pmatrix} \cdot \begin{pmatrix} I_n & O_n \\ T_f & ZH_f \end{pmatrix}.
\end{aligned}$$

Note that

$$\begin{aligned}
\det \begin{pmatrix} I_n & O_n \\ T_f & ZH_f \end{pmatrix} &= \det(I_n) \cdot \det(Z \cdot H_f) = \det(Z) \cdot \det(H_f) \\
&= (-1)^n \cdot \det(H_f^{\mathrm{t}}) = (-1)^n \cdot (a_n)^n \neq 0
\end{aligned}$$

and that

$$\begin{aligned}\det\begin{pmatrix} O_n & I_n \\ Z & T_f + ZH_g \end{pmatrix} &= \det\begin{pmatrix} O_n & I_n \\ Z & T_f + ZH_g \end{pmatrix} \\ &= \det\begin{pmatrix} O_n & I_n \\ Z & T_f \end{pmatrix} \cdot \det\begin{pmatrix} I_n & H_g \\ O_n & I_n \end{pmatrix} \\ &= \det(T_f) \cdot \det(I_n T_f^{-1} Z) \cdot 1 \neq 0\end{aligned}$$

Therefore, we conclude that

$$\text{nullity}(B) = \text{nullity}\begin{pmatrix} B & O_n \\ O_n & I_n \end{pmatrix} = \text{nullity}(R_{f,g}).$$

□

Theorem 76 together with Theorem 78 are called Jacobi-Darboux Theorem.

Remark. If we are given two polynomials $p, q \in \mathbb{C}[x, y]$ and we are asked to find all solutions to the equation

$$p(x, y) = 0, \qquad q(x, y) = 0.$$

We can use the following method. Fix y and we obtain two polynomials p_y and q_y with coefficients in $\mathbb{C}$. Then, (x_0, y_0) is a solution if $\det(B_{p_{y_0}, q_{y_0}}) = 0$.

3.2 Markov chain and the Perron-Frobenius Theorem

We first look at the following question:

> Suppose there are only two towns in the NTU Country, called the MATH town and the CSIE town. Suppose in every year, there are s% people from MATH moving to CSIE; and t% people from CSIE moving to MATH. Assume that there are no people died and born and no people moving out of the NTU Country. Then, we want to ask whether the population in these two towns will become steady.

Let S be the total population of the NTU country, and let p_k and q_k be the percentage of the total population in two towns MATH and CSIE, respectively, at the k-th year. Write $v_k = (p_k, q_k)^{\mathrm{t}}$. Then, we have

$$v_{k+1} = \begin{pmatrix} 1 - s\% & t\% \\ s\% & 1 - t\% \end{pmatrix} v_k$$

Define

$$M := \begin{pmatrix} 1 - s\% & t\% \\ s\% & 1 - t\% \end{pmatrix},$$

then we wonder whether the limit

$$\lim_{k \to \infty} v_k = \lim_{k \to \infty} M v_k$$

exists? Above discussions give us the motivation to study Markov chain. The next two definitions are helpful for us rephrasing the problem.

Definition 79 (Steady state)**.** Given a matrix $M \in M_n(\mathbb{R})$, a steady state $v \in \mathbb{R}^n$ is an eigenvector of M with eigenvalue 1, namely, $M \cdot v = v$.

Definition 80 (Stochastic matrix)**.** Suppose $M \in M_n(\mathbb{R})$. $M = (m_{ij})$ is called a stochastic matrix if all its entries are nonnegative and

$$\sum_{i=1}^{n} m_{ij} = 1,$$

for all $j \in [1, n]$.

We restate the problem as *"Is the steady state of a stochastic matrix exists and is unique up to a scalar?"* In general, the answer is "no". For instance, let $M = I_n$, then every state is a steady state. So, our goal is to find the sufficient condition when the steady state is unique.

Definition 81 (Positive matrix and non-negative matrix)**.** Given a matrix $M \in M_n(\mathbb{R})$.

1. M is positive (non-negative) if all its entries are positive (non-negative). We often write $M > 0$ or $M \geq 0$.
2. M is regular if M is non-negative and M^k is positive for some $k \in \mathbb{N}$. (The terminology "Regular" is sometimes confusing.)

Theorem 82. *Let $M \in M_n(\mathbb{R})$ be a stochastic matrix. If M is regular then a steady state of M is unique up to a scalar. In other words,* $\dim \ker(M - I_n) = 1$.

In fact, there is a more stronger result, however we shall introduce some other terminologies first.

Definition 83 (Spectral radius)**.** Let $A \in M_n(\mathbb{C})$ and let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be all the eigenvalues of A (roots of the characteristic polynomial). The spectral radius of A is defined as

$$\rho(A) := \max_{1 \leq i \leq s} |\lambda_i| .$$

Hence, we have $\rho(A) \geq 0$.

The stronger result mentioned above is the next theorem, which is proved by Oskar Perron (1907) and Georg Frobenius (1912).

Theorem 84 (Perron-Frobenius Theorem)**.** *Let $A \in M_n(\mathbb{R})$ be a regular matrix. Then, there exists a unique (up to a scalar) eigenvector $v \in \mathbb{R}^n$ with eigenvalue $\rho(A)$.*

Note that we does not assume $\rho(A)$ is an eigenvalue. Therefore, this theorem is pretty strong. Since it requires a lot of work to prove Theorem 84, we shall prove some theorems and lemmas first, instead.

Theorem 85 (Gelfond's formula)**.** *Let $A \in M_n(\mathbb{C})$. Then,*

$$\rho(A) = \lim_{k\to\infty} \left\|A^k\right\|^{1/k}.$$

Although this theorem is regard as a lemma of Theorem 84, we still need to decompose it into some small problems.

Lemma 12. Let A and B be two similar complex matrices. That is, there exists an invertible matrix $P \in M_n(\mathbb{C})$ such that

$$A = P^{-1}BP.$$

Then,

$$\lim_{k\to\infty} \left\|A^k\right\|^{1/k} = \lim_{n\to\infty} \left\|B^k\right\|^{1/k},$$

provided that $\lim \left\|A^k\right\|^{1/k}$ exists.

Proof. Let $t = \|P\| \cdot \left\|P^{-1}\right\| \geq \left\|P \cdot P^{-1}\right\| = 1$. Then,

$$\left\|A^k\right\| = \left\|P^{-1} \cdot B^k \cdot P\right\| \leq \left\|P^{-1}\right\| \cdot \left\|B^k\right\| \cdot \|P\| = t \cdot \left\|B^k\right\|.$$

Similarly, we have

$$\left\|B^k\right\| \leq t \cdot \left\|A^k\right\|.$$

We conclude

$$t^{-1/k} \left\|A^k\right\|^{1/k} \leq \left\|B^k\right\|^{1/k} \leq t^{1/k} \left\|A^k\right\|^{1/k}.$$

Taking the limit $k \to \infty$, we obtain $\lim \left\|A^k\right\|^{1/k} = \lim \left\|B^k\right\|^{1/k}$. □

Proof of Theorem 85. If x is an eigenvector of eigenvalue λ, then

$$\begin{aligned} \left|A^k x\right| = |\lambda|^k \cdot |x| &\implies \left\|A^k\right\| \geq |\lambda|^k \\ &\implies \left\|A^k\right\|^{1/k} \geq |\lambda|. \end{aligned}$$

We find $\left\|A^k\right\|^{1/k} \geq \rho(A)$ for all $k \in \mathbb{N}$. It remains to prove that $\lim \left\|A^k\right\|^{1/k}$ exists and

$$\rho(A) \geq \lim_{k\to\infty} \left\|A^k\right\|^{1/k}.$$

From what we have learnt in the theory of Jordan forms and Lemma 12, we just need to consider the case when A is of Jordan form. We first consider the case when A is a Jordan block J_λ, that is,

$$A = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix} = \lambda \cdot I_n + N \in M_n(\mathbb{C}),$$

where $N = J_0$. Then,

$$A^k = (\lambda \cdot I_n + N)^k = \sum_{i=0}^{k} \binom{k}{i} \lambda^{k-i} N^i = \sum_{i=0}^{n} \binom{k}{i} \lambda^{k-i} N^i \qquad (\text{if } k \geq n)$$

If we assume $k \geq n$, we then have

$$\left\|A^k\right\| = \left\| \sum_{i=0}^{n} \binom{k}{i} \lambda^{k-i} N^i \right\| \leq \sum_{i=0}^{n} \binom{k}{i} |\lambda|^{k-i} = |\lambda|^k \cdot p(k),$$

where

$$p(k) = \sum_{i=0}^{n} |\lambda|^{-i} \binom{k}{i}$$

is a polynomial in k. Thus,

$$\left\|A^k\right\|^{1/k} \leq |\lambda| \cdot p(k)^{1/k} \to |\lambda| .$$

Estimations above show that the theorem is true when A is a Jordan block. Now, we claim that if

$$A = B \oplus C = \begin{pmatrix} B & \\ & C \end{pmatrix},$$

then $\|A\| = \max\{\|B\| , \|C\|\}$. This claim proves the theorem, since $\left\|A^k\right\|^{1/k}$ converge to $\max_{1 \leq i \leq s}\{|\lambda_i|\}$ when

$$A = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix}, \ J_i \text{ are all Jordan blocks.}$$

We now start proving the claim. Let $B \in M_p(\mathbb{C})$ and $C \in M_q(\mathbb{C})$ and let $a = \max\{\|B\| , \|C\|\}$. Observe that for all $x \in \mathbb{C}^p$ and $y \in \mathbb{C}^q$, we have

$$\left\| \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right\| = \sqrt{|Bx|^2 + \left|Cy\right|^2} \leq \sqrt{a^2 \cdot (|x| + \left|y\right|)}.$$

Hence, we conclude that

$$\left\| \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \right\| \leq a.$$

On the other hand, there exist $x_0 \in \mathbb{C}^p$ and $y_0 \in \mathbb{C}^q$ such that

$$\left|Bx_0\right| = \|B\| \cdot \left|x_0\right| , \qquad \left|Cy_0\right| = \|C\| \cdot \left|y_0\right| .$$

Then, we have

$$\left\| \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} x_0 \\ 0 \end{pmatrix} \right\| \leq \|B\| \cdot \left\| \begin{pmatrix} x_0 \\ 0 \end{pmatrix} \right\|, \qquad \left\| \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} 0 \\ y_0 \end{pmatrix} \right\| \leq \|C\| \cdot \left\| \begin{pmatrix} 0 \\ y_0 \end{pmatrix} \right\|,$$

this proves the theorem. □

Theorem 86. *Let $A \in M_n(\mathbb{R})$ be a positive real matrix. The following statements are true.*

1. *There is a positive vector $u \in \mathbb{R}^n_{>0}$ such that $A \cdot u = \rho(A)u$.*
2. *If $v \in \mathbb{C}^n$ is an eigenvector of A with eigenvalue λ satisfying $|\lambda| = \rho(A)$, then $\lambda = \rho(A)$.*
3. *The algebraic multiplicities of $\rho(A)$ is 1.*

Proof. Let $v \in \mathbb{C}^n$ be an eigenvector of A with eigenvalue λ satisfying $|\lambda| = \rho(A)$. Write $v = \begin{pmatrix} v_1 & v_2 & \dots & v_n \end{pmatrix}^{\mathrm{t}} \in \mathbb{C}^n$ and let $w = \begin{pmatrix} |v_1| & |v_2| & \dots & |v_n| \end{pmatrix}^{\mathrm{t}} \in \mathbb{R}^n_{\geq 0}$. We claim that $A \cdot w = \rho(A) \cdot w$. Note that

$$(Aw)_i = \sum_{j=1}^{n} a_{ij} w_j = \sum_{j=1}^{n} a_{ij} |v_j| \geq \left| \sum_{j=1}^{n} a_{ij} v_j \right| = |(Av)_i| = |\lambda v_i| = \rho(A) |v_i| = \rho(A) w_i.$$

If $Aw \neq \rho(A)w$, then $A \cdot Aw > A \cdot \rho(A)w$, that is, all components of $A \cdot Aw$ are strictly greater than those of $A \cdot \rho(A)w$. It is possible to choose $\epsilon > 0$ such that

$$A \cdot Aw \geq (1 + \epsilon) A \cdot \rho(A)w.$$

By induction, we get:

$$A^{k+1} w \geq \Big((1 + \epsilon)\rho(A) \Big)^k \cdot Aw, \text{ for all } k \in \mathbb{N}.$$

This implies that

$$\left\| A^k \right\| \geq \frac{\left| A^k \cdot (Aw) \right|}{|Aw|} \geq \Big((1 + \epsilon)\rho(A) \Big)^k \implies \left\| A^k \right\|^{1/k} \geq (1 + \epsilon)\rho(A),$$

contradicting the Gelfond's formula (Theorem 85). Hence, $Aw = \rho(A)w$. However, from the definition of w, we have $w \geq 0$, therefore we conclude that $w > 0$. This proves the first assertion. To see the second statement, observe that

$$\sum_{j=1}^{n} \left| a_{ij} v_j \right| = \sum_{j=1}^{n} a_{ij} \left| v_j \right| = |\lambda v_i| = \left| \sum_{j=1}^{n} a_{ij} v_j \right|, \text{ for all } i.$$

This implies all v_i have the same argument (principal value), that is, $\arg(v_i)$ are the same. Here we have used a cool fact about the complex number.

> Let $c_1, c_2, \dots, c_n \in \mathbb{C} \setminus \{0\}$. Then
>
> $$|c_1 + c_2 + \cdots + c_n| = |c_1| + |c_2| + \cdots + |c_n|$$
>
> implies $c_1, c_2, \dots, c_n$ have the same principal values (arguments).

Since all v_i have the same principle value, we may assume that $v_i = r_i \cdot \exp(i\theta)$ ($r_i \in \mathbb{R}_{\geq 0}$) for all $1 \leq i \leq n$.

Thus, we have

$$\lambda \cdot \begin{pmatrix} r_1 \exp i\theta \\ r_2 \exp i\theta \\ \vdots \\ r_n \exp i\theta \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} r_1 \exp i\theta \\ r_2 \exp i\theta \\ \vdots \\ r_n \exp i\theta \end{pmatrix} = \exp(i\theta) \begin{pmatrix} \sum a_{1j} r_j \\ \sum a_{2j} r_j \\ \vdots \\ \sum a_{nj} r_j \end{pmatrix}$$

$$\implies \lambda \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = A \cdot \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} \sum a_{1j} r_j \\ \sum a_{2j} r_j \\ \vdots \\ \sum a_{nj} r_j \end{pmatrix} \text{ is a real matrix.}$$

Hence, this shows that λ is real, thus proves the second assertion. It remains to prove the third statement. Since $A > 0$, $A^{\mathrm{t}} > 0$. We can apply (1.) and (2.) to A^{t}. Let $x \in \mathbb{R}^n_{>0}$ be an eigenvector of A^{t} with eigenvalue $\rho(A^{\mathrm{t}}) = \rho(A)$. Consider

$$X := \{y \in \mathbb{R}^n : x^{\mathrm{t}} \cdot y\} \subset \mathbb{R}^n.$$

Note the following facts:

1. X is an A-invariant subspace. ($\because x^{\mathrm{t}} \cdot Ay = (A^{\mathrm{t}}x)^{\mathrm{t}} y = \rho(A) x^{\mathrm{t}} y = 0$, for all $y \in X$.)
2. $w \notin X$. $\Big($Recall that $v = \begin{pmatrix} v_1 & v_2 & \dots & v_n \end{pmatrix}^{\mathrm{t}}$ and $w = \begin{pmatrix} |v_1| & |v_2| & \dots & |v_n| \end{pmatrix}^{\mathrm{t}}$ is an eigenvector of A with eigenvalue $|\lambda| = \rho(A)$.$\Big)$

Thus, $\mathbb{R}^n = X \oplus \mathbb{R} \cdot w$. To show the algebraic multiplicity of $\rho(A)$ is 1, it suffices to show that there is no eigenvectors in X with eigenvalue $\rho(A)$. Let $y \in X$ with $Ay = \rho(A)y$. Then from the prove of (1.), it follows that

$$Ay^* = \rho(A)y^*, \text{ where } y_i^* = \left|y_i\right|.$$

We saw that the components of $A(y + y^*)$ is either all zeros or all positive (why?). This indicates $y^* = \pm y$. However, $\langle y^*, x \rangle > 0$ contradicting the definition of X. This completes the proof. □

Corollary. Let $A \in M_n(\mathbb{R})$ be a regular matrix. Suppose A^k is positive. Then, The following statements are true.

1. There is a positive vector $u \in \mathbb{R}^n_{>0}$ such that $A \cdot u = \rho(A)u$.
2. If $v \in \mathbb{C}^n$ is an eigenvector of A with eigenvalue λ satisfying $|\lambda| = \rho(A)$, then $\lambda = \rho(A)$.
3. The algebraic multiplicities of $\rho(A)$ is 1.

Proof. Let $\mathrm{Ev}(A)$ be the multiset of all eigenvalues of A in $\mathbb{C}$ counted with multiplicity. In other words,

$$\mathrm{Ev}(A) = \text{the multiset of roots of } \mathrm{ch}_A(x).$$

If $\mathrm{Ev}(A) = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$, then $\mathrm{Ev}(A^k) = \{\lambda_1^k, \lambda_2^k, \dots, \lambda_n^k\}$ (from the theory of the Jordan forms). Hence, $\rho(A^k) = \rho(A)^k$. Without loss of generality, we assume that $|\lambda_1| = \rho(A)$, and we will

write λ for λ_1. By Theorem 86, $\lambda^k \in \mathbb{R}_{>0}$ and there exists $u \in \mathbb{R}^n_{>0}$ such that

$$A^k u = \lambda^k u.$$

Let $v \in \mathbb{C}^n$ be an eigenvector of A with eigenvalue λ. Then, v is an eigenvector of A^k with eigenvalue λ^k. Theorem 86 asserts that v and u differ a scalar in $\mathbb{C}$. Thus, u is an eigenvector of A and

$$Au = \lambda u.$$

On the left side is a positive vector, so λ is a positive real number. ($\because \rho(A) \neq 0$, otherwise $A^k = 0$ for large enough k.) This proves the first statement.

To see the second statement, let $w \in \mathbb{C}^n$ be an eigenvector of A with eigenvalue μ satisfying $\left|\mu\right| = \rho(A) = \lambda$. Then,

$$A^k w = \mu^k w, \qquad \left|\mu^k\right| = \rho(A^k).$$

By (2.) and (3.) of Theorem 86, we have

$$\mu^k = \rho(A^k),$$

and w and u differ scalar. This means that w is an eigenvector of A with eigenvalue $\rho(A)$.

It remains to show the third statement. From $\left|\lambda^k\right| > \left|\lambda_i^k\right|$ for all $1 < i \leq n$, it follows that $|\lambda| > |\lambda_i|$. This proves the last assertion. □

Theorem 86 and its corollary is actually a stronger result of Theorem 84. This theorem has a generalization to irreducible matrix. We now formally give the following definition.

Definition 87 (Irreducible matrix)**.** A non-negative matrix is A is irreducible matrix if for any $1 \leq i, j \leq n$, there exist k (depending on i, j) such that

$$\left\langle A^k e_i, e_j \right\rangle > 0,$$

where $\{e_1, e_2, \ldots, e_n\}$ is the standard basis of $\mathbb{R}^n$ and $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^n$.

Theorem 88. *Let $A \in M_n(\mathbb{R})$ be an irreducible matrix. Then the following statements are true.*

1. *There is a positive vector $u \in \mathbb{R}^n_{>0}$ such that $A \cdot u = \rho(A)u$.*
2. *The algebraic multiplicities of $\rho(A)$ is 1.*

Remark. This generalization does not claim the following:

> Let $v \in \mathbb{C}^n$ be an eigenvector of A with eigenvalue λ satisfying $|\lambda| = \rho(A)$. Then, $\lambda = \rho(A)$.

Here gives a counterexample. Let $A \in M_2(\mathbb{R})$ be an non-negative matrix defined by:

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that A is irreducible but NOT regular, however, ± 1 are both eigenvalues of A.

Proof of Theorem 88. From the definition of irreducible matrices, for every $1 \leq i \leq n$ and $1 \leq j \leq n$, there exists $k = k(i,j) \in \mathbb{N}$ such that

$$\left\langle A^k e_i, e_j \right\rangle > 0.$$

We now let $k_0 = \max_{(i,j)} k(i,j) \in \mathbb{N}$. Then, $(A + \epsilon I_n)^{k_0}$ is positive for all $\epsilon > 0$. Let $\mathrm{Ev}(A) = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$ be the sorted multiset of eigenvalues of A, that is, we assume

$$\rho(A) = |\lambda_1| = |\lambda_2| = \cdots = |\lambda_s| > |\lambda_{s+1}| \geq \cdots \geq |\lambda_n|.$$

We claim that there exists an $\epsilon > 0$ being small enough such that

$$|\lambda_r + \epsilon| = \rho(A + \epsilon I_n) \text{ and } |\lambda_r| = \rho(A), \text{ for some } 1 \leq r \leq s.$$

We show that all ϵ in the interval $\left((|\lambda_s| - |\lambda_{s+1}|)/4\right)$ satisfies the requirement. Let $1 \leq p \leq s$ and $s < q \leq n$ be two integers. Then,

$$\left|\lambda_p + \epsilon\right| \geq \left|\lambda_p\right| - \epsilon > \left|\lambda_q\right| + \epsilon \geq \left|\lambda_q + \epsilon\right|.$$

This means $\rho(A + \epsilon I_n) = |\lambda_r|$ for some $r \in [1, s]$.

By Theorem 86 and its corollary, $\lambda_r + \epsilon \in \mathbb{R}_{>0}$ and there exists an $u \in \mathbb{R}^n_{>0}$ such that

$$(A + \epsilon I_n)u = (\lambda_r + \epsilon)u \implies Au = \lambda_r u.$$

Au is a non-negative vector and $|\lambda_r| = \rho(A) \neq 0$, thus $\lambda_r = \rho(A) \in \mathbb{R}_{>0}$. This proves the first assertion.

To see the second assertion, suppose

$$\mathrm{ch}_A(x) = (x - \lambda_r) \prod_{i \neq r} (x - \lambda_i).$$

Then,

$$\mathrm{ch}_{(A+\epsilon I_n)}(x) = (x - \lambda_r - \epsilon) \prod_{i \neq r} (x - \lambda_i - \epsilon).$$

By the corollary of Theorem 86 again, $(x - \lambda_i - \epsilon) \neq (x - \lambda_r - \epsilon)$ for all $i \neq r$. This completes the proof. □

Definition 89 (Perron-Frobenius vector)**.** Let $A \in M_n(\mathbb{R})$ be an irreducible matrix. Let v_A be the unique vector in $\mathbb{R}^n_{>0}$ such that

$$Av_A = \rho(A)v_A \text{ and } \sum_{i=1}^{n} v_i = 1,$$

where v_i are the i-th component. v_A is called the Perron-Frobenius vector, or briefly, P-F vector.

3.3 Directed Graphs with Weights and Matrices

Definition 90 (Directed graphs with weights)**.** A (directed) graph is an ordered pair $G = (V, E)$, where V is called the vertex set and E is called the set of edges. The vertex set $V = \{v_\alpha : \alpha \in \Lambda\}$ consists of some vertices, in the subsection, we assume that $|V|$ is finite. The set

of edges E consists of some pairs (v_i, v_j) $(i, j \in \Lambda)$, meaning that there is an edge from v_i to v_j. A directed graph with weights means that we require the set of edges E consists of some triples (v_i, v_j, w_{ij}), meaning that there is an edge from v_i to v_j with weight $w_{ij} \in \mathbb{R}_{>0}$.

Note that for each directed graph with weights, we can associate it with a non-negative matrix by the following

Suppose $|V| = n$. Let $A_G = (a_{ij}) \in M_n(\mathbb{R})$ be a non-negative matrix defined by

$$a_{ij} = \begin{cases} w_{ji} & \text{, if } (v_j, v_i, w_{ji}) \in E \\ 0 & \text{, otherwise} \end{cases}.$$

Then, for each finite directed graph G with weights, we associate it with a non-negative matrix A_G, the adjacency matrix of G. We also can construct a graph from a given non-negative matrix. Thus, some properties of the matrix theory can convert to properties of graphs, and vice versa.

Now let G be an unweighted directed graph, for each vertex, we can define the out-degree and in-degree as

$$\deg_{\text{out}}(v) = \#\{w \in V : (v, w) \in E\}; \quad \deg_{\text{in}}(v) = \#\{w \in V : (w, v) \in E\}.$$

We can construct a related matrix $S = (s_{ij}) \in M_n(\mathbb{R})$ corresponding to the transitions in a Markov chain of given network N (a net work is an unweighted directed graph G), by

$$s_{ij} = \begin{cases} \dfrac{1}{\deg_{\text{out}}(v_j)} & \text{, if } (v_j, v_i) \in E \\ 0 & \text{, if } (v_j, v_i) \notin E \text{ but } \deg_{\text{out}}(v_j) \neq 0 \\ \dfrac{1}{n} & \text{, otherwise} \end{cases}.$$

Then, the just constructed matrix S is a stochastic matrix, but it may not be regular or irreducible. To make S be able to apply Theorem 84, we give the following definition of the google matrix that makes S become positive.

Definition 91 (Google matrix)**.** Let N be a network (let G be a unweighted directed graph). The google matrix X attached to the network N (the graph G) is

$$X := \alpha S + (1 - \alpha)\frac{1}{n}B, \text{ for some } \alpha \in (0, 1). \tag{7}$$

In (7), B is defined as the matrix in $M_n(\mathbb{R})$, all of whose elements are 1. Usually, $\alpha = 0.85$ is the best model for simulating how people browse the web page according to the research by Google at around 1997.

The Google matrix X is positive and stochastic. We can apply the Perron-Frobenius Theorem (Theorem 84) to X to get a P-F vector $v_X = \begin{pmatrix} v_1 & v_2 & \dots & v_n \end{pmatrix}^{\text{t}}$. Then, we (Google) can rank web pages in Google search engine results according to the magnitude of v_i. However, how to find v_X is a very tricky question. Most of the time, there are a lot of pages to be ranked, so we must find a quick way to compute v_X numerically.

Theorem 92. *Let* $v_0 = \begin{pmatrix} 1/n & 1/n & \dots & 1/n \end{pmatrix}^{\mathrm{t}} \in \mathbb{R}^n$. *Then,*

$$\lim_{k\to\infty} X^k v_0 = v_X.$$

Proof. For $x \in \mathbb{R}^n$, define

$$\|x\|_1 := \sum_{i=1}^{n} |x_i| .$$

For any $v = \begin{pmatrix} v_1, v_2, \dots, v_n \end{pmatrix}^{\mathrm{t}} \in \mathbb{R}^n_{\geq 0}$ such that $\sum v_i = 1$, we have

$$B \cdot v = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}^{\mathrm{t}}.$$

In this case, we call v a probability vector. Let $v_k = X^k v_0$ $(k \in \mathbb{N})$. Consider $\|v_k - v_X\|_1$.

$$\|v_k - v_X\|_1 = \left\| \left(\alpha S + (1-\alpha)\frac{1}{n}B\right)(v_{k-1} - v_X) \right\|_1 = \|(\alpha S)(v_{k-1} - v_X)\|_1 ,$$

because v_{k-1} and v_X are probability vectors. Define $x^{(k)} := v_k - v_X$. Then, $x^{(k+1)} = \alpha \cdot S \cdot x^{(k)}$. Note that

$$\begin{aligned} \left\|x^{(k+1)}\right\|_1 &= \sum_{i=1}^{n} \left|x_i^{(k+1)}\right| \leq \alpha \sum_{i=1}^{n} \sum_{j=1}^{n} s_{ij} \left|x_j^{(k)}\right| \\ &= \alpha \sum_{j=1}^{n} \sum_{i=1}^{n} s_{ij} \left|x_j^{(k)}\right| = \alpha \sum_{j=1}^{n} \left|x_j^{(k)}\right| = \alpha \cdot \left\|x^{(k)}\right\|_1 . \end{aligned}$$

This implies

$$\left\|x^{(k)}\right\|_1 \leq \alpha^k \cdot \left\|x^{(0)}\right\|_1 = \alpha^k \cdot \left\|v_0 - v_X\right\|_1 \leq 2\alpha^k.$$

We obtain

$$\lim_{k\to\infty} v_k = v_X.$$

□

Corollary. We have $\left\|X^k v_0 - v_X\right\| \leq 2 \cdot \alpha^k$, It is useful when we need to estimate the error between $X^k v_0$ and v_X.

This method to approximate the exact value of v_X is called the power method. We now consider a more general question. Given a positive stochastic matrix $A \in M_n(\mathbb{R})$ and let v_0 be a vector in $\mathbb{R}^n$, then we wonder whether the limit $\lim A^k v_0$ exists and what the limit is. The answer is given by the next theorem.

Theorem 93. *Let A be a positive matrix. Let $w, v_A \in \mathbb{R}^n$ be the P-F vectors of A^{t} and A, respectively. Let $v \in \mathbb{R}^n$ be an arbitrary vector, then*

$$\lim_{k\to\infty} \left(\frac{A}{\rho(A)}\right)^k v = \frac{\langle v, w\rangle}{\langle v_A, w\rangle} \cdot v_A,$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product.

Proof. Recall that in the proof of the Theorem 86, we used the fact that

$$\mathbb{R}^n = (\mathbb{R} \cdot v_A) \oplus W \quad (W := (\mathbb{R} \cdot w)^\perp = \{x \in \mathbb{R}^n : \langle x, w \rangle = 0\}),$$

is a direct sum of A-invariant subspace of $\mathbb{R}^n$. For each $v \in \mathbb{R}^n$, write $v = \alpha v_A + y$, where $y \in W$. Then,

$$\begin{aligned}
\left(\frac{A}{\rho(A)}\right)^k \cdot v - \alpha v_A &= \left(\frac{A}{\rho(A)}\right)^k \cdot (v - \alpha v_A) = \left(\frac{A}{\rho(A)}\right)^k \cdot y \\
\implies \left|\left(\frac{A}{\rho(A)}\right)^k \cdot v - \alpha v_A\right| &= \left|\left(\frac{A}{\rho(A)}\right)^k \cdot y\right| \leq \left(\frac{1}{\rho(A)^k}\right) \cdot \left\|(A|_W)^k\right\| \cdot |y| \\
&< C \cdot \left(\frac{\rho(A|_W)}{\rho(A)}\right)^k \cdot |y| \quad \text{(by Gelfond's formula).}
\end{aligned}$$

Since $\rho(A) > \rho(A|_W)$ (by Theorem 86), we have

$$\lim_{k\to\infty} \left(\frac{A}{\rho(A)}\right)^k \cdot v = \alpha \cdot v_A.$$

On the other hand, we have

$$\langle v, w \rangle = \langle \alpha v_A + y, w \rangle = \alpha \langle v_A, w \rangle \implies \alpha = \frac{\langle v, w \rangle}{\langle v_A, w \rangle}.$$

This proves the theorem. □

Remark. This theorem does not hold if A is an irreducible matrix since we use the fact that

> If A is positive (non-negative), then $\rho(A) > \rho(A|_W)$. (W is the orthogonal complement of $\mathbb{R} \cdot v_A$.)

Acknowledgement

這篇文章首先要感謝我的老師謝明倫教授，提供他在 2016 授課的影片，也感謝網路上豐富的資源，以及閱讀過這篇文章的同學，尤其是幫助我改進錯誤的! 最後我則是要感謝自己約一至兩個月的辛苦努力，相信這份筆記在未來是對自己是有許多幫助的!!

First of all, I would like to thank my teacher, Prof. Ming-Lun Hsieh, for providing the video of his class in 2016, as well as the rich resources on the internet and the students who have read this article, especially for helping me to improve my mistakes! Finally, I would like to thank myself for the hard work I have put in for about one to two months, and I believe this note will be of great help to me in the future!

References

[1] Pete L. Clark. "QUADRATIC FORMS CHAPTER I : WITT'S THEORY". In: 2010.

[2] S.H. Friedberg, A.J. Insel, and L.E. Spence. *Linear Algebra*. Featured Titles for Linear Algebra (Advanced) Series. Pearson Education, 2003. ISBN: 9780130084514.

[3] 謝銘倫. 線性代數二. https://www.youtube.com/playlist?list=PLVJXJebpO4PgW5WgeU_hIml7mSO8Eoggx. 2016.