

The Real (serious) 245 \{Tensor Product\} Notes

Letian Chen

Dec 2, 2015

Contents

1	Stochastic Process	2
1.1	Matrix Limit	2
1.2	Stochastic Matrices	3
2	Spaces and Linear Transformations	5
2.1	Matrix Representation of a Linear Map	5
2.2	Direct Sums	5
2.3	Quotient Spaces	6
2.4	Quotient Spaces and Invariant Subspaces	7
2.5	Dual Spaces	8
2.6	Free Vector Space	10
3	Canonical Forms	11
3.1	Cayley-Hamilton Theorem and Minimal Polynomial	11
3.2	Block Diagonalization	14
3.3	The Rational Canonical Form	16
3.4	Jordan Canonical Form	20
4	Bilinear Forms and Orthogonal Diagonalization	24
4.1	Inner Product Space	24
4.2	Orthogonality	27
4.3	The Hermitian Adjoint	31
4.4	Normal Operators	35
4.5	Unitary Matrices	38
4.6	Bilinear Forms over Other Fields	41
5	Tensor Algebra	46

1 Stochastic Process

1.1 Matrix Limit

Insert reviews here, I did not take notes for those. I was an idiot. I thought he was Stephen Newish.

Definition 1.1 (Matrix Limit). Let $A_i \in M_{n \times n}(\mathbb{R})$, $i \in \mathbb{N}$ and $L \in M_{n \times n}(\mathbb{R})$, we say $\lim_{n \rightarrow \infty} A_n = L$ if and only if $\lim_{n \rightarrow \infty} (A_n)_{ij} = L_{ij}$.

Definition 1.2 (Matrix Exponential). We define the **matrix exponential** as

$$\exp(A) = \sum_{k=0}^{\infty} \frac{1}{k!} A^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n \frac{1}{k!} A^k$$

Theorem 1.3. The matrix exponential is well-defined; that is, the limit exists.

Proof. Let $\|A\|_{\infty} = \max\{A_{ij}\}$ be the infinity norm of matrix A . We proceed by induction on k to show that

$$\left| \left(\frac{1}{k!} A^k \right)_{ij} \right| \leq \frac{n^{k-1}}{k!} \|A\|_{\infty}^k \quad (1)$$

This is obvious for $k = 1$. Now assume the claim holds for $k = m$, then for $k = m + 1$, we have

$$\begin{aligned} \left| \left(\frac{1}{(m+1)!} A^{m+1} \right)_{ij} \right| &= \left| \frac{1}{m+1} \left(\frac{1}{m!} A^m A \right)_{ij} \right| \leq \left| \frac{1}{m+1} \|A\|_{\infty} \sum_{k=1}^n \left(\frac{1}{m!} A^m \right)_{ik} \right| \\ &\leq \frac{1}{m+1} \|A\|_{\infty} \left(\frac{n^{m-1}}{m!} \|A\|_{\infty}^m \right) \cdot n \\ &= \frac{n^m}{(m+1)!} \|A\|_{\infty}^{m+1} \end{aligned} \quad (2)$$

where the last inequality comes from the induction hypothesis, and we see the claim holds true for $k = m + 1$. Hence the claim holds for all k , as desired. Therefore it suffices to show the convergence of the series

$$\sum_{k=0}^{\infty} \frac{n^{k-1}}{k!} \|A\|_{\infty}^k \quad (3)$$

By the ratio test, we have

$$\lim_{k \rightarrow \infty} \frac{n^k}{(k+1)!} \|A\|_{\infty}^{k+1} \left(\frac{n^{k-1}}{k!} \|A\|_{\infty}^k \right)^{-1} = \lim_{k \rightarrow \infty} \frac{n \|A\|_{\infty}}{k+1} = 0 \quad (4)$$

Therefore the series converges, and by the comparison test, the limit exists as well. \square

There are two subsequent applications of this definition, one of them being solving systems of differential equations.

Consider $y_1(t), y_2(t), \dots, y_n(t) \in C^1(\mathbb{R})$ such that

$$\begin{cases} y_1'(t) &= a_{11}y_1(t) + a_{12}y_2(t) + \dots + a_{1n}y_n(t) \\ &\vdots \\ y_n'(t) &= a_{n1}y_1(t) + a_{n2}y_2(t) + \dots + a_{nn}y_n(t) \end{cases} \quad (5)$$

We can let $\vec{y}(t) = (y_1(t), y_2(t), \dots, y_n(t))^t$ and A be the matrix with $A_{ij} = a_{ij}$, then the system can be rewritten as

$$\frac{d\vec{y}(t)}{dt} = A\vec{y}(t) \quad (6)$$

Recall the solution for the linear first-order differential equation $y' = ay$, the solution has the form of $y(t) = y(0)e^{at}$, and we have the following

Magic 1.4. *This works for $\vec{y}(t)$ as well!*

Therefore the general solution to the above system is $\vec{y}(t) = e^{At}\vec{y}(0)$. It remains to calculate $\exp(A)$. This will be easy if A is diagonalizable. Suppose $D = Q^{-1}AQ$ for some invertible Q , then we have easily, by letting $D_{ii} = \lambda_i$,

$$\exp(At) = \sum_{k \geq 0} \frac{1}{k!} (At)^k = \sum_{k \geq 0} \frac{1}{k!} Q D^k t^k Q^{-1} = Q \left(\sum_{k \geq 0} \frac{D^k t^k}{k!} \right) Q^{-1} = Q D' Q^{-1}, \quad (7)$$

where

$$D' = \begin{pmatrix} e^{\lambda_1 t} & 0 & \cdots & 0 \\ 0 & e^{\lambda_2 t} & & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{\lambda_n t} \end{pmatrix}$$

The second application will be introduced in the next section.

1.2 Stochastic Matrices

Definition 1.5 (Probability Vector). *A vector $(x_1, \dots, x_n)^t \in \mathbb{R}^n$ is a **probability vector** if $\sum_{i=1}^n x_i = 1$.*

Definition 1.6 (Stochastic Matrix). *A matrix A is **stochastic** if every column of A is a probability vector*

Remark. Some other texts define this in terms of row vectors. Moreover, a matrix is doubly stochastic if every column and row vector is a probability vector.

Remark. If A is a stochastic matrix, so is A^m .

Definition 1.7 (Markov Chain). *A **Markov Chain** is a random process satisfying the following conditions*

- *There are n states, namely $1, 2, \dots, n$*
- *Each step transforms one state to another*
- *A_{ij} denotes the probability of going from state j to i*
- *The probability does not change at each step*

where A is the stochastic matrix associated with the process.

Remark. Note that A_{ij} is the probability from j to i , not the other way around.

Markov Chain is one of the most important concept in stochastic process in statistics, which nobody cares about. Also, nobody cares about Chris either. The following concerns about the theory of stochastic matrices. We first introduce two Lemmas. Let $S = \{\lambda \in \mathbb{C} \mid |\lambda| < 1\} \cup \{1\}$.

Lemma 1.8. *Let $A \in M_{n \times n}(\mathbb{R})$, then $\lim_{m \rightarrow \infty} A^m$ exists if the following hold*

1. *Every eigenvalue of A belongs to S*
2. *If 1 is an eigenvalue of A then $\dim E_1 = \text{mult}(1)$*

Lemma 1.9. *Let $A \in M_{n \times n}(\mathbb{R})$, and λ an eigenvalue of A , then the following are equivalent*

1. *$\text{mult}(\lambda) > \dim E_\lambda$*
2. *there exists non-zero vectors $x, y \in \mathbb{R}_{\text{col}}^n$ such that $Ax = \lambda x$ and $Ay = \lambda y + x$*

Unfortunately we are unable to prove these two lemmas at this point (of life), but these will be proved once we build up more machinery, i.e. Jordan Canonical Form.

Next we introduce the concept of a regular stochastic matrix.

Definition 1.10. A stochastic matrix A is **regular** if some power of A has all entries non-zero.

Proposition 1.11. If A is a regular stochastic matrix, then

1. every eigenvalue of A belongs to S
2. 1 is an eigenvalue of A , and $\text{mult}(1) = \dim E_1 = 1$
3. there is a unique probability vector $x \in E_1$ such that $\lim_{m \rightarrow \infty} A^m = (x \ x \ \dots \ x)$

Proof. Let λ be an eigenvalue of A , then $Ax = \lambda x \implies A^s x = \lambda^s x$. Since A is stochastic, $\|A^s\|_\infty \leq 1$. Therefore

$$|\lambda^s| \|x\|_\infty = \|A^s x\|_\infty \leq \|A^s\|_\infty \|x\|_\infty \implies |\lambda^s| \leq 1 \ \forall s \geq 1 \quad (8)$$

Hence $\lambda \leq 1$ and $\lambda \in S$. Next, to show that 1 is an eigenvalue of A , simply notice that $e = (1 \ 1 \ \dots \ 1)$ satisfies $eA = e$ and thus is a left-eigenvector of A . Thus 1 is an eigenvalue of A . Next we show that if $|\lambda| = 1$, then $\lambda = 1$. Let $v \in \mathbb{R}_{\text{row}}^n$ be a left-eigenvector; that is, $vA = \lambda v$. Let $\{e_1, e_2, \dots, e_n\}$ be the standard basis for $\mathbb{R}_{\text{col}}^n$. Then we write $v = (v_1 \ v_2 \ \dots \ v_n)$ where $v_j = v e_j$.

By the definition of the infinity norm, $|v_j| \leq \|v\|_\infty$ for all $j = 1, 2, \dots, n$ and there exists k such that $|v_k| = \|v\|_\infty$. Since for all $s \geq 1$, $vA^s = \lambda^s v$, we have

$$\|v\|_\infty = |v_k| = |\lambda^s v_{e_k}| = |vA^s e_k| = \left| \sum_{j=1}^n v_j (A^s)_{jk} \right| \leq \|v\|_\infty \sum_{j=1}^n (A^s)_{jk} = \|v\|_\infty \quad (9)$$

The equality holds if and only if $|v_i| = \|v\|_\infty$ for all $i = 1, 2, \dots, n$. Therefore $v = v_k (1 \ 1 \ \dots \ 1) \implies \lambda = 1$

Next we show that $\text{mult}(1) = \dim E_1$. Suppose the contrary that $\text{mult}(1) > \dim E_1$, then by Lemma 1.9 there exists non-zero vectors $x, y \in \mathbb{R}_{\text{col}}^n$ such that $Ax = x$ and $Ay = x + y$. So it follows that $A^s y = sx + y$ for all $s \geq 1$, and the following holds

$$s\|x\|_\infty - \|y\|_\infty \leq \|sx + y\|_\infty = \|A^s y\|_\infty \leq n\|A^s\|_\infty \|y\|_\infty \leq n\|y\|_\infty \quad (10)$$

which means that $\|x\|_\infty \leq \frac{n+1}{s} \|y\|_\infty \ \forall s \geq 1$, which is equivalent to $\|x\|_\infty = 0$, contradiction.

Finally, since $AL = A \lim_{m \rightarrow \infty} A^m = \lim_{m \rightarrow \infty} A^{m+1} = L$, every column of L is in E_1 , since L is stochastic, the result follows. \square

2 Spaces and Linear Transformations

2.1 Matrix Representation of a Linear Map

Note that in this course, we are majorly interested in finite dimensional vector spaces, although many of the definitions do generalize to infinite dimensional vector spaces.

Let V and W be two vector spaces over \mathbb{F} , let $\beta = \{v_1, v_2, \dots, v_n\}$ be a basis for V and $\gamma = \{w_1, w_2, \dots, w_m\}$ a basis for W . If $v \in V$ is represented as $v = \sum_{i=1}^n b_i v_i$, we define $[v]^\beta$ to be $(b_1, b_2, \dots, b_n)^t$.

Furthermore, if $T \in \mathcal{L}(V, W)$ and $T_{v_j} = \sum_{i=1}^m a_{ij} w_i$, we define

$$[T]_\beta^\gamma = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

To simplify the notation, we introduce a new operator Ψ .

Magic 2.1. Let $\Psi_\beta = (v_1 \ v_2 \ \dots \ v_n)$, we have the following alternative definitions for $[v]^\beta$ and $[T]_\beta^\gamma$:

$$\begin{aligned} v &= \Psi_\beta [v]^\beta \\ T\Psi_\beta &= \Psi_\gamma [T]_\beta^\gamma \end{aligned}$$

Remark. Note that this complicated definition indeed simplifies the notation by around π .

Remark. This unintentionally complicated notation gives rise of the following identities, which do not involve Ψ at all.

$$\begin{aligned} [T]_\beta^\gamma [v]^\beta &= [Tv]^\gamma \\ [u]_\gamma^\delta [v]^\beta &= [uv]_\beta^\delta \end{aligned}$$

The above notation allows us to transform abstract linear algebra to concrete matrix algebra, in fact,

$$\begin{aligned} \ker T &= \{\Psi x \mid x \in \text{Null}([T]_\beta^\gamma)\} \\ \text{Im } T &= \{\Psi y \mid y \in \text{Col}([T]_\beta^\gamma)\} \end{aligned}$$

We also have the change of basis formula for a linear map. In fact, if $\beta' = \{v'_1, v'_2, \dots, v'_n\}$ and $\gamma' = \{w'_1, w'_2, \dots, w'_m\}$ bases for V and W respectively, we can write $\Psi_{\beta'} = \Psi_\beta Q_1$ and $\Psi_{\gamma'} = \Psi_\gamma Q_2$ for some Q_1 and Q_2 , then the change of basis formula is given by

$$[T]_{\beta'}^{\gamma'} = Q_2 [T]_\beta^\gamma Q_1^{-1}$$

It shall be pointed out that diagonalization is nothing but a special case of the above formula, with $T \in \mathcal{L}(V)$ and D a diagonal matrix with $T\Psi_\beta = \Psi_\beta D$.

2.2 Direct Sums

Definition 2.2 (Direct Sum). Let V, W be two vector spaces over \mathbb{F} , the direct sum $V \oplus W$ is defined to be the vector space associated with two linear maps $i_1 : V \rightarrow V \oplus W$, $i_2 : W \rightarrow V \oplus W$ such that every $x \in V \oplus W$ can be expressed uniquely as $x = i_1(v) + i_2(w)$ where $v \in V$ and $w \in W$.

We demonstrate in the next two example that this definition is indeed correct.

Example. The (conventional) internal direct sum defined as $X = V \oplus W \iff X = V + W \wedge V \cap W = \emptyset$ is a well-defined direct sum as in the above definition with $i_1(v) = v$ and $i_2(w) = w$ for $v \in V$ and $w \in W$.

Example. The (conventional) external direct sum defined as $V \oplus W = \{(v, w) | v \in V, w \in W\}$ is a well-defined direct sum as in the above definition with $i_1(v) = (v, 0)$ and $i_2(w) = (0, w)$ for $v \in V$ and $w \in W$.

Remark. Notice that our spectacular definition of direct sum can be generalized to more than 2 vector spaces easily, while the Cartesian product is no longer the correct way to construct the external direct sums

Whats more to our extraordinarily magnificent definition is that it provides a simple tool to find a basis for $V \oplus W$. In fact, if β is a basis for V and γ a basis for W , then it follows directly $i_1(\beta) \cup i_2(\gamma)$ is a basis for $V \oplus W$.

Proof. If that is not obvious to you, you can either go home and think about it or consider arranging an appointment with Kevin Purbhoo. \square

2.3 Quotient Spaces

Roughly speaking, a quotient space is the opposite to a subspace. Recall that a subspace of a vector space V is a vector space W that comes with an injective linear map $i : W \rightarrow V$, called the inclusion map, given by $i(w) = w$ for $w \in W$. Therefore to construct a quotient space, it is natural to consider instead of an injective map, a surjective map. This leads us to the following definition.

Definition 2.3 (Quotient Space). A **quotient space** of V is a subspace X associated with a surjective map $\pi : V \rightarrow X$, called the quotient map. If we let $W = \ker \pi$, we call X the quotient of V by W , and write $X = V/W$ (reads $V \bmod W$).

Remark. Alternatively, we shall use the following notation of the surjective map more frequently. If W is a subspace of V , the quotient of V by W , denoted V/W , is a vector space associated with a surjective linear map $\pi_{V/W} : V \rightarrow V/W$ and $\ker \pi_{V/W} = W$.

Remark. Note that I have substituted the word “come with” in the definition to “associated with” to increase the formality.

One may also notice the conventional construction of a quotient space $V/W = \{v + W | v \in V\}$, where $v + W = \{v + w | w \in W\}$. This can be easily verified to satisfy the definition of a vector space. This definition gives an explicit formula of our surjective map mentioned above, namely $\pi_{V/W} = v + W$.

As we have constructed the subspace, we may want to dissect it a little further. In fact, we have the following results.

Proposition 2.4. If V is a finite dimensional vector space, $W \subset V$, then

$$\dim V/W = \dim V - \dim W$$

Proof. Since $\ker \pi_{V/W} = W$, by the rank-nullity theorem, $\dim \ker \pi_{V/W} + \text{rank } \pi_{V/W} = \dim V$. Rearrange to get $\dim V/W = \text{rank } \pi_{V/W} = \dim V - \dim W$. \square

The next proposition concerns about basis for V/W .

Proposition 2.5. If $\{w_1, w_2, \dots, w_l\}$ is a basis for W , $\{v_1, \dots, v_m\} \subset V$, then $\{v_1 + W, \dots, v_m + W\}$ is a basis for V/W if and only if $\{w_1, \dots, w_l, v_1, \dots, v_m\}$ is a basis for V .

Proof. First we assume that $\{v_1 + W, \dots, v_m + W\}$ is a basis for V/W . Assume the contrary that $\{w_1, \dots, w_l, v_1, \dots, v_m\}$ is not linearly independent, then there exists a non-trivial linear combination that gives 0, i.e.

$$\sum_{i=1}^l a_i w_i + \sum_{i=1}^m a_{l+i} v_i = 0 \tag{1}$$

Notice that $w = \sum_{i=1}^l a_i w_i \in W$, then there is a linear combination

$$\sum_{i=1}^m a_{l+i} v_i = -w \in \ker \pi_{V/W} \implies \sum_{i=1}^m a_{l+i} (v_i + W) = W = \ker \pi_{V/W} \quad (2)$$

contradiction.

Conversely, assume $\{w_1, \dots, w_l, v_1, \dots, v_m\}$ is a basis for V . Assume the contrary that $\{v_1 + W, \dots, v_m + W\}$ is not linearly independent, i.e. there exists a non-trivial linear combination

$$\sum_{i=1}^m a_{l+i} (v_i + W) = W \implies \sum_{i=1}^m a_{l+i} v_i \in W \implies \sum_{i=1}^m a_{l+i} v_i = \sum_{j=1}^l a_j w_j \quad (3)$$

which is equivalent to a linear combination

$$\sum_{i=1}^l a'_i w_i + \sum_{i=1}^m a_{l+i} v_i = 0 \quad (4)$$

with $a'_i = -a_i$ for $1 \leq i \leq l$, contradiction. \square

Next we demonstrate further how quotient spaces are related to subspaces. Let $T : V \rightarrow V'$ be a linear map. The question we want to ask for a subspace is that, can you restrict the domain or the codomain of T to a smaller subspace. It is obvious that we can do this for the domain, as we can use $T \circ i : W \rightarrow V'$ where i is the inclusion map from W to V . Things are a little bit more complicated for the codomain, (omitting 100 words), and as it turns out, we can do so if and only if there exists a linear map $\tilde{T} : V \rightarrow W' \subset V'$ such that $T = i \circ \tilde{T}$. This \tilde{T} is also unique, if it exists.

The case for the quotient space is exactly the opposite. To replace the co-domain, we only need to use the quotient map to get $\pi_{V/W} \circ T : V \rightarrow V'/W'$. For the domain we need some condition similar to the one above. (Omitting 100 words), the conclusion is that we can do so if and only if there exists a surjective linear map $\bar{T} : V/W \rightarrow V'$ such that $T = \bar{T} \circ \pi_{V/W}$ for some $W \in \ker T$. This is a totally non-obvious fact.

In fact, if \bar{T} exists, then for $w \in W$, $T(w) = \bar{T} \circ \pi_{V/W}(w) = \bar{T}(0) = 0 \implies W \subset \ker T$.

On the other hand, if $W \subset \ker T$, we can construct \bar{T} as the following. For $\bar{x} \in V/W$, choose $x \in V$ such that $\pi_{V/W}(x) = \bar{x}$. Note such x exists due to surjectivity. It remains to verify that \bar{T} is well-defined. In fact, $\pi_{V/W}(x) - \pi_{V/W}(x') = 0 \implies \pi_{V/W}(x - x') = 0 \implies x - x' \in \ker \pi_{V/W} = W \implies \bar{T}(x - x') = 0 \implies \bar{T}(x) = \bar{T}(x')$. Finally, if \bar{T} exists, it is unique, since $\pi_{V/W}$ is surjective.

2.4 Quotient Spaces and Invariant Subspaces

Definition 2.6 (Invariant Subspace). *Let $T \in \mathcal{L}(V)$ be a linear operator and W a subspace of V . We say W is **T -invariant** if $Tw \in W$ for all $w \in W$.*

Roughly speaking, if a subspace is T -invariant, then the image under T still lies in the subspace.

Example. Any subspace spanned by T -eigenvectors is T -invariant, by definition.

Example. If W is a T -invariant subspace, then so is $\text{im } W$.

If W is T -invariant, there are two natural linear maps that come with the property.

$$\begin{aligned} T_W : W &\rightarrow W, \quad T_W(w) = Tw \\ \bar{T}_{V/W} : V/W &\rightarrow V/W, \quad \bar{T}_{V/W}(x + W) = Tx + W \end{aligned}$$

The first map is generally referred as T restricted to W , and it can be used for the question of replacing codomain with subspace mentioned in the last section, since $\text{im } T_W \subset W$. Similarly, the second map can be

used to replace the domain with quotient space in the last section, since $W \subset \ker \bar{T}_{V/W}$, and if that is not obvious to you, you know what to do.

With the knowledge of T -invariant subspaces, we are able to establish some deep¹ results. The following theorem shows that, by choosing a T -invariant subspace of V , the matrix representation of a linear operator is essentially block upper-triangular.

Theorem 2.7. *Let V be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$ and $W \subset V$ a T -invariant subspace. Suppose $\gamma = \{w_1, w_2, \dots, w_l\}$ is a basis for W and $\beta = \{w_1, \dots, w_l, v_1, \dots, v_m\}$ is a basis for V . Let $\bar{\beta} = \{v_1 + W, \dots, v_m + W\}$, then $[T]_\beta = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ is block upper-triangular, for some $A \in M_{l \times l}(\mathbb{F})$, $B \in M_{l \times m}(\mathbb{F})$ and $C \in M_{m \times m}(\mathbb{F})$. Moreover, $A = [T_W]_\gamma$ and $C = [\bar{T}_{V/W}]_{\bar{\beta}}$.*

Proof. Since W is T -invariant, we have

$$T(w_1 \dots w_l) = (w_1 \dots w_l)A \quad (5)$$

$$T(v_1 \dots v_m) = (w_1 \dots w_l)B + (v_1 \dots v_m)C \quad (6)$$

For some $A \in M_{l \times l}(\mathbb{F})$, $B \in M_{l \times m}(\mathbb{F})$ and $C \in M_{m \times m}(\mathbb{F})$. Combining (5) and (6) yields

$$T(w_1, \dots, w_l, v_1, \dots, v_m) = (w_1 \dots w_l \ v_1 \dots v_m) \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \quad (7)$$

which is equivalent to $[T]_\beta = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$.

(5) directly implies that $A = [T_W]_\gamma$. To see $C = [\bar{T}_{V/W}]_{\bar{\beta}}$, we have

$$\begin{aligned} \bar{T}_{V/W}(v_1 + W \dots v_m + W) &= \pi_{V/W} \circ T(v_1 \dots v_m) \\ &= \pi_{V/W}(w_1 \dots w_l)B + \pi_{V/W}(v_1 \dots v_m)C \\ &= (v_1 + W \dots v_m + W)C \end{aligned} \quad (8)$$

where the second equality comes from (6) and $(w_1 \dots w_l) \in \ker \pi_{V/W}$, and the proof is complete. \square

There are many things we can do by putting T into upper-triangular form, we can compute the determinant much more easily, and more importantly, $f_T(t) = f_{T_W}(t)f_{\bar{T}_{V/W}}(t)$. We will be using this result later as well.

2.5 Dual Spaces

Definition 2.8 (Dual Space). *Let V be a vector space over \mathbb{F} . The **Dual Space** to V is $V^* = \mathcal{L}(V, \mathbb{F})$.*

The following is a non-obvious example.

Example. $\mathbb{F}_{\text{col}}^n = (\mathbb{F}_{\text{row}}^n)^*$. To see this consider a row acting on a column, the product is exactly the dot product, which is in \mathbb{F} .

In general, we have $\dim V^* = \dim V$, only if V is finite dimensional. In fact, when V is finite dimensional, we see that $\beta^* = \{f_1(x), \dots, f_n(x)\}$ is indeed a basis for V^* , where $\beta = \{v_1, \dots, v_n\}$ is a basis for V and

$$f_i(v_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

¹Some mathematicians see beauty in mathematical results that establish connections between two areas of mathematics that at first sight appear to be unrelated. These results are often described as deep. See Mathematical Beauty in Wikipedia for more information.

Moreover for each β , β^* is unique and is called the dual basis of V^2 . If $x \in V$, and $g \in V^*$, then obviously $g(x) \in \mathbb{F}$, and less obviously $x(g) \in L(V)$. More importantly, the following identity holds for dual basis.

$$\sum_{i=1}^n v_i f_i = I_v \quad (9)$$

Recall that $\Psi_\beta = (v_1 \dots v_n)$. If we associate $\Psi^\beta = (f_1 \dots f_n)^t$, we see that they are mutually inverse.

Next few results concern about duality.

Theorem 2.9 (Double Dual Theorem). *Let V be a vector space over \mathbb{F} and V^* the dual of V . Then V^{**} is the dual of V^* and there exists a natural injective linear map $\varphi : V \rightarrow V^{**}$ given by $\varphi(x)(f) = f(x)$ for all $x \in V$ and $f \in V^*$. Moreover if V is finite-dimensional, this is an isomorphism and $V = V^{**}$.*

Proof. φ is clearly linear. To see that it is also injective, we check $\ker \varphi$. Indeed, $\varphi(x) = 0 \iff f(x) \equiv 0 \iff x = 0$. The rest follows. \square

Theorem 2.10 (Transpose). *Let V, W be finite dimensional vector spaces over \mathbb{F} . Let $T \in L(V, W)$. There exists a map $T^t \in L(W^*, V^*)$ called the transpose of T , satisfying for all $g \in W^*$ and $v \in V$,*

$$(T^t g)v = g(Tv) \quad (10)$$

Moreover, if β and γ are bases for V and W respectively and β^*, γ^* the corresponding dual bases, then $[T^t]_{\gamma^*}^{\beta^*} = \left([T]_{\beta}^{\gamma}\right)^t$.

Proof. It is easy to verify that the above map is linear. It remains to show $[T^t]_{\gamma^*}^{\beta^*} = \left([T]_{\beta}^{\gamma}\right)^t$. Let $\beta = \{v_1, \dots, v_n\}$, $\gamma = \{w_1, \dots, w_m\}$, $\beta^* = \{f_1, \dots, f_n\}$ and $\gamma^* = \{g_1, \dots, g_m\}$. The the j th column of $[T^t]_{\gamma^*}^{\beta^*}$ is

$$T^t(g_j) = g_j T = \sum_{i=1}^n (g_j T) v_i f_i \quad (11)$$

and it follows that

$$\left([T^t]_{\gamma^*}^{\beta^*}\right)_{ij} = (g_j T)(v_i) = g_j(T(v_i)) = g_j \left(\sum_{k=1}^m \left([T]_{\beta}^{\gamma}\right)_{ki} w_k \right) = \sum_{k=1}^m \left([T]_{\beta}^{\gamma}\right)_{ki} g_j(w_k) = \left([T]_{\beta}^{\gamma}\right)_{ji} \quad (12)$$

since all terms for which $k \neq j$ vanish. Therefore $[T^t]_{\gamma^*}^{\beta^*} = \left([T]_{\beta}^{\gamma}\right)^t$, as desired. \square

Remark. It is easy to see that the transpose T^t is unique, and the proof is very straightforward.

Remark. It is also true that $(T^t)^t = T$, and if T is injective, T^t is surjective.

Next we introduce the concept of an annihilator.

Definition 2.11 (Annihilator). *Let V be a finite dimensional vector space, $W \subset V$. The **annihilator** of W is define to be the set*

$$W^\circ = \{f \in V^* \mid f(w) = 0 \ \forall w \in W\}$$

There exist a few non-obvious identity of the annihilator. They are totally non-obvious.

Proposition 2.12. *Let V be a finite dimensional vector space, $W, X \subset V$. We have the following identities:*

1. $(W^\circ)^\circ = W$
2. $(W \cap X)^\circ = W^\circ + X^\circ$

²This fact appears as a theorem in his notes

3. $(W + X)^\circ = W^\circ \cap X^\circ$
4. $(V/W)^* = W^\circ$
5. $W^* = V^*/W^\circ$

Proof. To see 1, recall that

$$(W^\circ)^\circ = \{f \in V^{**} \mid f(w) = 0 \ \forall w \in W^\circ\} \quad (13)$$

Then, using the same map φ in Theorem 2.9, we have, for $w \in W^\circ$,

$$\varphi(x)(w) = w(x) = 0 \iff x \in W \quad (14)$$

and that is $W = (W^\circ)^\circ$.

To see 2, let $f \in W^\circ + X^\circ$ be expressed as $f = f_w + f_x$ where $f_w \in W^\circ$ and $f_x \in X^\circ$, then for any $a \in W \cap X$, $f(a) = f_w(a) + f_x(a) = 0 \implies (W^\circ + X^\circ) \subset (W \cap X)^\circ$. On the other hand, let $f \in (W \cap X)^\circ$, then we define $f_w \in W^\circ$ as

$$f_w(x) = \begin{cases} 0 & x \in W \\ f(x) & x \notin W \wedge x \in X \\ \frac{f(x)}{2} & x \notin W \cup X \end{cases} \quad (15)$$

and similarly $f_x \in X^\circ$, it can be verified that $f = f_w + f_x$ indeed and hence $(W \cap X)^\circ = W^\circ + X^\circ$. A similar argument can be used to prove 3.

To see 4, consider the linear map $\pi : V^* \rightarrow W^*$ given by $\pi(f) = f \circ i$, where $i : W \rightarrow V$ is the inclusion map. It is easy to verify that π is linear. We claim that π is also surjective.

Since i is injective, there exists a left-inverse of i , call j , such that $j \circ i = I$. Consider $\bar{\pi} : W^* \rightarrow V^*$ given by $\bar{\pi}(g) = g \circ j$, we have

$$\pi \circ \bar{\pi}(g) = \bar{\pi}(g) \circ i = g \circ j \circ i = g \quad (16)$$

Thus $\bar{\pi}$ is a right inverse of π , and hence π is surjective. Now $\ker \pi$ is the set that sends all function $f \in V^*$ to f' for which $f'(w) = 0$ for $w \in W$, namely $\ker \pi = W^\circ$. Recall the definition of a quotient space, we can write this as $W^* = V^*/W^\circ$. A similar argument can be used to prove 5, with the map $j : (V/W)^* \rightarrow V^*$ given by $j(\bar{f}) = \pi_{V/W} \circ \bar{f}$ where $\pi_{V/W}$ is the quotient map. \square

Remark. I confess that I was trying to avoid to prove 5 which is the hardest among them all.

The following concepts have never been used in the course so far, and we shall not prove it.

Definition 2.13 (Cokernel and Coimage). Let V, W be vector spaces and $T \in \mathcal{L}(V, W)$, the **cokernel** of T is $\text{coker } T = W/\text{im } T$ and the **coimage** of T is $\text{coim } T = V/\ker T$.

Proposition 2.14. Let V, W be vector spaces and $T \in \mathcal{L}(V, W)$, then

$$\begin{aligned} (\ker T)^* &= \text{coker } T^t \\ (\text{im } T)^* &= \text{coim } T^t \end{aligned}$$

Proof. I will add them when I am in the mood. \square

2.6 Free Vector Space

This section is used in tensor products.

Definition 2.15. Let S be a set, the **free vector space** $\text{Free}(S)$ over a field \mathbb{F} is a vector space for which $S \subseteq \text{Free}(S)$ is a basis.

Example. If $S = \{s_1, s_2, s_3, s_4\}$, then $\text{Free}(S)$ is a 4-dimensional vector space over \mathbb{F} , and S is a basis, namely

$$\text{Free}(S) = \{as_1 + bs_2 + cs_3 + ds_4 \mid a, b, c, d \in \mathbb{F}\}$$

Notice that in the case $S \subset \mathbb{F}$ we will get some trouble in the notations, and they can be fixed either by creating new notations for elements in S or new notations for operator in $\text{Free}(S)$.

Free vector spaces also have the adjoint property, which states that if V is any vector space over \mathbb{F} and $f : S \rightarrow V$ is any function, then there exists a unique linear map $\bar{f} : \text{Free}(S) \rightarrow V$ extending f . Whatever, this has not been used in the course so far.

3 Canonical Forms

Our ultimate goal in this section is to decompose a linear operator T into block diagonal blocks so that each of the block cannot be decomposed further.

3.1 Cayley-Hamilton Theorem and Minimal Polynomial

If V is a vector space over \mathbb{F} and $T \in \mathcal{L}(V)$, then for a polynomial

$$p(t) = \sum_{i=0}^n a_i t^i$$

we write

$$p(T) = \sum_{i=0}^n a_i T^i$$

which is also a linear operator.

Also we introduce cyclic subspaces, a special case of an invariant subspace.³

Definition 3.1. Let V be a vector space, $T \in \mathcal{L}(V)$. For $x \in V$, the ***T-cyclic subspace*** generated by x is

$$X = \text{Span}\{x, Tx, T^2x, \dots\}$$

Remark. The T-cyclic subspace generated by x is also the smallest T-invariant subspace that contains x .

Proposition 3.2. Let V be a finite dimensional vector space, $T \in \mathcal{L}(V)$, and X the T-cyclic subspace generated by x . If $\dim X = k$, then $\beta = \{x, Tx, \dots, T^{k-1}x\}$ is a basis for X . Moreover $[T_X]_\beta$ is a companion matrix.

Proof. Let m be the smallest integer such that there exists a nontrivial linear combination

$$\sum_{i=0}^m a_i T^i x = 0 \tag{1}$$

Clearly $m \leq k$. If $m < k$, we proceed by induction to show that $T^i x$ can be written as a linear combination of $\{x, Tx, \dots, T^{m-1}x\}$ for $i \geq m$. This is clear for $i = m$. Assume the claim is true for $i = n$, then for $i = n + 1$,

$$T^{n+1}x = T(T^n x) = T\left(\sum_{i=0}^{m-1} b_i T^i x\right) = \sum_{i=1}^m b_i T^i x \tag{2}$$

The last sum is clearly a linear combination of $\{x, Tx, \dots, T^{m-1}x\}$, and by induction, the claim holds for all $i \geq m$. By definition of X , $\dim X = m < k$, contradiction.

³This was first introduced in an assignment, to make the note complete I decide to include it.

Recall the definition of a companion matrix at the very beginning (not here), we have, for $0 \leq i \leq k-1$, the i th column of $[T_X]_\beta$ is the vector with 1 at the $i+1$ -th entry and 0 everywhere else, since $T(T^i x) = T^{i+1}x$. For the last column, notice that there is a linear combination

$$T(T^{k-1}x) = T^k x = \sum_{i=0}^{k-1} a_i T^i x \quad (3)$$

and therefore the last column would be $(a_0 \dots a_{k-1})^t$. Hence

$$[T_X]_\beta = \begin{pmatrix} 0 & 0 & \cdots & a_0 \\ 1 & 0 & \cdots & a_1 \\ 0 & 1 & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{k-1} \end{pmatrix} \quad (4)$$

which is exactly the companion matrix. \square

Theorem 3.3 (Cayley-Hamilton Theorem). *If V is a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$, then $f_T(T) \equiv 0_V$.*

Proof. This proof is not credited to Stephen New. Let $x \in V$, consider W , the T -cyclic subspace generated by x . Let $k = \dim W$, so it follows from Proposition 3.2 that $\gamma = \{x, Tx, \dots, T^{k-1}x\}$ is a basis for W . Therefore we have

$$T^k x = \sum_{i=0}^{k-1} b_i T^i x \quad (5)$$

for some $b_i \in \mathbb{F}$. By Proposition 3.2 again, $[T_W]_\gamma$ is a companion matrix, and therefore

$$f_{T_W}(t) = t^k - \sum_{i=0}^{k-1} b_i t^i \quad (6)$$

It follows from (5) that

$$f_{T_W}(T)x = 0 \quad (7)$$

Finally, since W is T -invariant, by Theorem 2.7, $f_T(t) = f_{T_W}(t)f_{\bar{T}_{V/W}}(t)$, and it follows $f_T(T)x \equiv 0$. \square

We have shown that the characteristic polynomial of a linear operator T annihilates T , but it is not necessarily the one with the lowest degree, for example the n by n identity map I_n , its characteristic polynomial is $f_I(t) = (t-1)^n$, while it is obvious that $g(t) = t-1$ would annihilate I . This leads us to the following definition:

Definition 3.4. *Let V be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$, the **minimal polynomial** is defined to be the unique monic polynomial $m_T(t) \in \mathbb{F}[t]$ such that $m_T(T)x = 0$ for all $x \in V$.*

Theorem 3.5. *The minimal polynomial is well-defined; that is, such polynomial exists and is unique.*

Proof. Notice by Cayley-Hamilton theorem, $f_T(T)x = 0$ for all $x \in V$, therefore we can take $m_T(t)$ to be the polynomial with the least degree. Hence the existence. To see the uniqueness, assume there exists another minimal polynomial $\tilde{m}_T(t)$, then $\deg(\tilde{m}_T(t) - m_T(t)) < \deg m_T(t)$, contradiction. \square

Theorem 3.6. *Let $p(t)$ be any polynomial such that $p(T) \equiv 0_V$, then $m_T(t) \mid p(t)$.*

Proof. Let $g(t)$ be $\gcd(p(t), m_T(t))$, then $\deg g(t) \leq \deg m_T(t)$. By the Euclidean Algorithm, there exist $a(t)$ and $b(t)$ such that

$$g(t) = a(t)p(t) + b(t)m_T(t) \implies g(T) = a(T)p(T) + b(T)m_T(T) \equiv 0 \quad (8)$$

Therefore, by the definition of minimal polynomial, $\deg g(t) \geq \deg m_T(t) \implies \deg g(t) = \deg m_T(t) \implies g(t) = m_T(t) \implies m_T(t) \mid p(t)$. \square

Corollary 3.7. *In particular, $m_T(t) \mid f_T(t)$, and if this is not obvious to you.*

We then have the following strong result to decompose kernel of $p(T)$ into smaller subspaces.

Theorem 3.8 (Primary Decomposition Theorem). *Let V be a vector space over \mathbb{F} , $T \in \mathcal{L}(V)$. Let $p(t) = \prod_{i=1}^k p_i(t)$ with $\gcd(p_i(t), p_j(t)) = 1$ for $i \neq j$. Then*

$$\ker p(T) = \bigoplus_{i=1}^k \ker p_i(T)$$

Proof. It is enough to prove this in the case $k = 2$, since we have $\ker p(T) = \ker p_1(T) \oplus \ker p_2(T)$, where $q(t) = \prod_{i=2}^k p_i(t)$. Induction on k does the rest.

Suppose $k = 2$, then $p(t) = p_1(t)p_2(t)$, let $W = \ker p(T)$. Take $x \in W$, we must show that

- i) $\ker p_i(T) \subset W$ for $i = 1, 2$
- ii) x can be written as $x = x_1 + x_2$ for $x_i \in \ker p_i(T)$
- iii) if $x \in \ker p_1(T) \cap \ker p_2(T)$ then $x = 0$

Since $\gcd(p_1(t), p_2(t)) = 1$, there exists $a_1(t)$ and $a_2(t)$ such that

$$a_1(t)p_1(t) + a_2(t)p_2(t) = 1 \quad (9)$$

Define linear operators P_1, P_2 on W by $P_2 = a_1(T)p_1(T)$ and $P_1 = a_2(T)p_2(T)$. It follows that

$$P_1x + P_2x = x \quad (10)$$

Then

- i) If $P_1(T)v = 0$ for $v \in V$, then $p(T)v = p_2(T)p_1(T)v = 0 \implies \ker p_i(T) \subset W$. Similarly for $p_2(t)$.
- ii) Let $x_1 = P_1(x)$, $x_2 = P_2(x)$. Then $x_1 + x_2 = x$ by (10). Also we have

$$P_1(T)x_1 = p_1(T)a_2(T)p_2(T)x_1 = a_2(T)p(T)x_1 = 0 \implies x_1 \in \ker p_i(t) \quad (11)$$

Similarly $x_2 \in \ker p_2(t)$

- iii) If $x \in \ker p_i(T) \cap \ker p_2(T)$, then

$$P_1(x) = a_2(T)p_2(T)x = 0 \quad (12)$$

Similarly $P_2(x) = 0$, and $x = P_1(x) + P_2(x) = 0$

And the proof is complete. □

Although this theorem seems very useless, it indeed gives us a criterion of diagonalizability.

Theorem 3.9. *Let V be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$, then T is diagonalizable over \mathbb{F} if and only if $m_T(t)$ is square-free and splits over $\mathbb{F}[t]$.*

Proof. Assume first that T is diagonalizable. Then there exists basis β for V such that $[T]_\beta = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ is diagonal. For any polynomial $p(t) \in \mathbb{F}[t]$, we have $[p(T)]_\beta = \begin{pmatrix} p(\lambda_1) & & \\ & \ddots & \\ & & p(\lambda_n) \end{pmatrix}$. This is not very obvious but if you go home and think about it, it should be obvious.

Let $S = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$ be the set of distinct eigenvalues of T . Clearly $p(T) \equiv 0_V \iff p(\lambda) = 0$ for all $\lambda \in S$. Therefore $m_T(t) = \prod_{i=1}^n (t - \lambda_i)$ is square-free and splits.

On the other hand, suppose $m_T(t) = \prod_{i=1}^n (t - \lambda_i)$, where λ_i is defined in the same way as above, then we apply the Primary Decomposition Theorem to $m_T(t)$ to get

$$V = \ker m_T(t) = \bigoplus_{i=1}^n \ker (T - \lambda_i I_V) = \bigoplus_{i=1}^n E_{\lambda_i} \quad (13)$$

Therefore $\dim V = \sum_{i=1}^n \dim E_{\lambda_i}$. Let β_i be a basis for E_{λ_i} , then $\beta = \bigcup_{i=1}^n \beta_i$ is a basis for V with T -eigenvectors, and $[T]_\beta$ is diagonal. \square

Remark. If $T \in \mathcal{L}(V)$ is a projection onto W (that is, $\text{im } T = W$ and $T^2 = T$), then T is diagonalizable, since $m_T(t) \mid t(t-1)$.

3.2 Block Diagonalization

In this section we will use our previous knowledge to put our matrix into a simpler form when it is not diagonalizable. First of all, we shall point out that this reduces to decompose a matrix into invariant subspaces, due to the following.

Proposition 3.10. *Let V be a finite dimensional vector space, $T \in \mathcal{L}(V)$. Then we can block diagonalize T with respect to a basis β such that*

$$[T]_\beta = \begin{pmatrix} [T_{W_1}]_{\beta_1} & & & & \\ & [T_{W_2}]_{\beta_2} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & [T_{W_n}]_{\beta_n} \end{pmatrix}$$

if and only if $T = \bigoplus_{i=1}^n W_i$ where W_i is T -invariant and $\beta = \bigcup_{i=1}^n \beta_i$ where β_i is a basis for W_i .

Proof. This follows from the definition of invariant subspaces. If this is not obvious to you, email kpurbo@uwaterloo.ca for more information. \square

With above in mind, it remains to check if we can actually decompose V into invariant subspaces. The rest of this section will answer this question.

Theorem 3.11. *Let V be a finite dimensional vector space, $L \in \mathcal{L}(V)$. Let $p(t) \in \mathbb{F}[t]$ be an irreducible polynomial. Then $q(t) \mid f_T(t)$ if and only if $\ker q(T) \neq \{0\}$.*

Proof. We first assume $q(t) \mid f_T(t)$. We proceed by induction on $\dim V$.

If $\dim V = 0$, the result is vacuously true. Now assume the result is true for $n < k$. For $n = k$, choose a non-zero vector $x \in V$, let W be the T -cyclic subspace generated by x . By Theorem 2.7, $f_T(t) = f_{T_W}(t)f_{\bar{T}_{V/W}}(t)$. Since $q(t)$ is irreducible, $q(t) \mid f_{T_W}(t)$ or $q(t) \mid f_{\bar{T}_{V/W}}(t)$.

If $q(t) \mid f_{T_W}(t)$, we can write $f_{T_W}(t) = q(t)h(t)$ for some $h(t) \in \mathbb{F}[t]$. Clearly $\deg h(t) < \dim W$. Therefore $h(T) \neq 0$. Pick $x \in W$ so that $h(T)x \neq 0$, it follows that $h(T)x \in \ker q(T)$ since $q(T)h(T)x = f_{T_W}(T)x = 0$ by the Cayley-Hamilton Theorem.

If $q(t) \mid f_{\bar{T}_{V/W}}$, by the hypothesis, the result is true for V/W . Then $\ker q(\bar{T}_{V/W}) \neq \{0\}$, so $q(\bar{T}_{V/W})$ is not invertible. Since $q(\bar{T}_{V/W}) = \overline{q(T)}_{V/W}$, it follows that $q(T)$ is not invertible. Hence $\ker q(T) \neq \{0\}$. Therefore the result is true for $n = k$. By induction, the result is true for all V .

On the other hand, if $\ker q(T) \neq \{0\}$, assume $q(t) \nmid f_T(t)$, then $\gcd(q(t), f_T(t)) = 1$, by the Primary Decomposition Theorem,

$$\ker q(T)f_T(t) = \ker q(T) \oplus \ker f_T(t) \implies V = \ker q(T) \oplus V \implies \ker q(T) = \{0\} \quad (14)$$

contradiction. \square

Remark. The non-obvious relation $q(\bar{T}_{V/W}) = \overline{q(T)}_{V/W}$ can be easily seen if you write $q(t)$ out.

Corollary 3.12. *Following in the definition from Theorem 3.11, if $g(t) \in \mathbb{F}[t]$ is any polynomial, then $g(T)$ is invertible if and only if $\gcd(g(t), f_T(t)) = 1$.*

Proof. Because of (14). This must be the shortest proof in the entire notes. \square

Then we have the following strong results to decompose V .

Theorem 3.13. *Let V be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$. Let $f_T(t) = \prod_{i=1}^k q_i(t)^{d_i}$, for which $\gcd(q_i(t), q_j(t)) = 1$ for $i \neq j$. Let $W_i = \ker q_i(T)^{d_i}$. Denote $T_i = T|_{W_i}$. Denote $f_i(t) = f_{T_i}(t)$ and $m_i(t) = m_{T_i}(t)$. Then*

1. $V = \bigoplus_{i=1}^k W_i$
2. $f_T(t) = \prod_{i=1}^k f_i(t)$
3. $f_i(t) = q_i(t)^{d_i}$
4. $\dim W_i = \deg q_i(t)^{d_i}$
5. $m_T(t) = \prod_{i=1}^k m_i(t)$
6. $m_i(t) = q_i(t)^{e_i}$ for some $1 \leq e_i \leq d_i$
7. $W_i = \{x \in V \mid q_i(T)^p x = 0 \text{ for some } p \geq 0\}$

Proof. 1. This follows directly from the Primary Decomposition Theorem, as

$$V = \ker f_T(T) = \bigoplus_{i=1}^k \ker q_i(T)^{d_i} = \bigoplus_{i=1}^k W_i \quad (15)$$

2. By Proposition 3.10, if β_i is a basis for W_i , then

$$[T]_{\beta} = \begin{pmatrix} [T_{W_1}]_{\beta_1} & & & \\ & [T_{W_2}]_{\beta_2} & & \\ & & \ddots & \\ & & & [T_{W_n}]_{\beta_n} \end{pmatrix}$$

Therefore $f_T(t) = \prod_{i=1}^k f_i(t)$.

3. By 2, the irreducible factors are divided amongst $f_i(t)$, therefore it suffices to show $q_j(t) \nmid f_i(t)$ for $i \neq j$. By Theorem 3.11, this is equivalent to $\ker q_j(T_i) = 0$. We have, since $\ker q_j(T) \subseteq \ker q_j(T)^{d_j} = W_j$,

$$\ker q_j(T_i) = \ker q_j(T) \cap W_i \subseteq W_j \cap W_i = \{0\} \implies \ker q_j(T_i) = \{0\} \quad (16)$$

as desired. Hence $f_i(t) = q_i(t)^{d_i}$.

4. By 3, $\dim W_i = \deg f_i(t) = \deg q_i(t)^{d_i}$.
 5. We first prove a lemma.

Lemma 3.14. *Let V be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$. If $V = \bigoplus_{i=1}^k W_i$ for W_i T -invariant, then $m_T(t) = \text{lcm}(m_1(t), m_2(t), \dots, m_k(t))$, where $m_i(t) = m_{T|_{W_i}}(t)$.*

Proof. It suffices to prove the case for $k = 2$, and induction does the rest. By Proposition 3.10, if β_1, β_2 are bases for W_1, W_2 respectively, $\beta = \beta_1 \cup \beta_2$ then $[T]_\beta$ is block diagonal. Let $w \in W_1$, then $m_1(t)w = m_T(t)w = 0 \implies m_1(t) \mid m_T(t)$. Similarly $m_2(t) \mid m_T(t)$, and therefore $\text{lcm}(m_1(t), m_2(t)) \mid m_T(t)$, by definition of the minimal polynomial $m_T(t) = \text{lcm}(m_1(t), m_2(t))$. \square

In this case, $\gcd(m_1(t), \dots, m_k(t)) = 1$, and therefore $m_T(t) = \prod_{i=1}^k m_i(t)$.

6. By Corollary 3.7, $m_T(t) \mid f_T(t) \implies e_i \leq d_i$. Since $\dim W_i \neq 0$, $m_i(t) \neq 1 \implies e_i \geq 1$.
 7. Clearly $W_i \subseteq \{x \in V \mid q_i(T)^p x = 0 \text{ for some } p \geq 0\}$. Now suppose $q_i(T)^p x = 0$. Let X be the T -cyclic subspace generated by x . Then $m_{T_X}(t) \mid q_i(t)^p \implies f_{T_X}(t) \mid q_i(t)^p$ because the minimal polynomial is precisely the characteristic polynomial in a cyclic subspace. Since $f_{T_X}(t) \mid f_T(t)$, $m_{T_X}(t) = q_i(t)^a$ for some $a \leq d_i$. Since $q_i(T)^a x = 0 \implies q_i(T)^{d_i} x = 0$, $x \in W_i$ as desired. Therefore $W_i = \{x \in V \mid q_i(T)^p x = 0 \text{ for some } p \geq 0\}$. \square

Remark. The minimal polynomial is precisely the characteristic polynomial in a cyclic subspace. To see this consider the basis $\beta = \{x, Tx, \dots, T^{\dim X - 1}x\}$ and the corresponding companion matrix. If this is still not obvious to you, you can either email snew@uwaterloo.ca or kpurbhoo@uwaterloo.ca.

The previous theorem ensures us that V can be put into direct sums of invariant subspaces, which means a linear operator is always block diagonalizable. This is essential, and is very close to our ultimate goal. The followings are terminologies which will be used later.

Definition 3.15 (Primary Subspace and Generalized Eigenspace). *Following the definitions in Theorem 3.13, $W_i = \ker q_i(T)^{d_i}$ are the **primary subspaces** of V under T .*

*If $d_i = 1$ for all i , the primary subspaces are called **generalized λ -eigenspaces** given by*

$$K_\lambda = \{x \in V \mid q_i(T)^p x = 0 \text{ for some } p \geq 0\}$$

Remark. Clearly $\dim K_\lambda = \text{mult}(\lambda)$, and if $f_T(t)$ splits, we have $V = \bigoplus_{\lambda} K_\lambda$.

3.3 The Rational Canonical Form

In the last section we established a method to decompose V into invariant subspaces. Recall our ultimate goal is to decompose V as much as we can. It turns out that it is not enough to only use Theorem 3.13, we can indeed decompose each W_i (as defined in Theorem 3.13) even further, into T -cyclic subspaces. In order to do so, we introduce 3 lemmas first. Let W be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(W)$. Let further $f_T(t) = q(t)^d$ where $q(t) \in \mathbb{F}[t]$ is irreducible. Denote $Z = \ker q(T)$.

Lemma 3.16. Let M_1, \dots, M_s be T -cyclic subspaces, then $W = \bigoplus_{i=1}^s M_i$ if and only if $\dim W = \sum_{i=1}^s \dim M_i$ and $Z = \bigoplus_{i=1}^s (M_i \cap Z)$.

Proof. Assume first that $W = \bigoplus_{i=1}^s M_i$, clearly $\dim W = \sum_{i=1}^s \dim M_i$ and

$$Z = Z \cap W = Z \cap \bigoplus_{i=1}^s M_i = \bigoplus_{i=1}^s (M_i \cap Z) \quad (17)$$

Conversely, we show that if $x_i \in M_i$ and $\sum_{i=1}^s x_i = 0$, then $x_i = 0$ for all i . Assume the contrary that $x_i \neq 0$ for some i , then there exists the largest integer p such that $q(T)^p x_i \neq 0$. By this definition, we have $q(T)^{p+1} x_j = 0$ for all j . Therefore $q(T)^p x_j \in \ker q(T) = Z$. It follows that $q(T)^p x_j \in Z \cap M_j$. But

$$\sum_{j=1}^s x_j = 0 \implies \sum_{j=1}^s q(T)^p x_j = 0 \quad (18)$$

together with $Z = \bigoplus_{i=1}^s (M_i \cap Z)$, $q(T)^p x_j = 0$ for all j , contradiction.

Since $\dim W = \sum_{i=1}^s \dim M_i$, we can conclude $W = \bigoplus_{i=1}^s M_i$. \square

Lemma 3.17. Let $Z' \subseteq Z = \ker q(T)$ be a T -invariant subspace. There exists T -cyclic subspaces X_1, \dots, X_k such that $Z = Z' \oplus \left(\bigoplus_{i=1}^k X_i \right)$.

Proof. If $Z' = Z$ we are done, otherwise we can choose $x \in Z \setminus Z'$. Consider X , the T -cyclic subspace generated by x . We show that $X \cap Z' = \{0\}$.

First of all, consider a T -invariant subspace X' of X . Let $\dim X' = m$ and $\dim X = n$. Then $\beta = \{x, Tx, \dots, T^{n-1}x\}$ is a basis for X by Proposition 3.2. Let $\{f_1(T)x, f_2(T)x, \dots, f_m(T)x\}$ be a basis for X' , let $g(t) = \gcd(f_1(t), \dots, f_m(t))$. By the extended Euclidean algorithm, $g(t) = \sum_{i=1}^m a_i(t)f_i(t)$ for some $a_i(t) \in \mathbb{F}[t]$. We show that $X' = \text{Span}\{g(T)x, Tg(T)x, \dots, T^{n-1}g(T)x\}$.

In fact, let $x' = \sum_{i=1}^m b_i f_i(T)x \in X'$, then

$$\sum_{i=1}^n a_i T^{i-1} g(T)x = x' = \sum_{i=1}^m b_i f_i(T)x \iff \sum_{i=1}^n a_i T^{i-1} x = \sum_{i=1}^m b_i d_i(T)x \quad (19)$$

where $f_i(t) = g(t)d_i(t)$. Since β is a basis for X and $\sum_{i=1}^m b_i d_i(T)x \in X$ there must exist such linear combination. Hence $X' = \text{Span}\{g(T)x, Tg(T)x, \dots, T^{n-1}g(T)x\}$, and it follows that X' is T -cyclic as well.

Next we show that $g(t) \mid q(t)$. Since $x \in Z'$, $q(T)x = 0$. Then there exists a linear combination

$$\sum_{i=1}^m a_i f_i(T)x = q(T)x = 0 \quad (20)$$

Since $g(t) \mid f_i(t)$ for all i , $g(t) \mid q(t)$ as desired.

Now, since X and Z' are both T -invariant, so is $X \cap Z'$. From the above argument, $X \cap Z'$ is T -cyclic as well, and is generated by $g(t) \mid q(t)$. But $q(t)$ is irreducible, so $g(t) = 1$ or $g(t) = q(t)$. If $g(t) = 1$, then $X \cap Z' = X$, which contradicts the choice of x (since $x \notin Z'$). Thus $g(t) = q(t)$ and $X \cap Z' = \{0\}$. Hence we can replace Z' by $Z' \oplus X$ and repeat the procedure until we get to the whole space Z . Call the T -cyclic subspaces X_1, X_2, \dots, X_k and we have $Z = Z' \oplus \left(\bigoplus_{i=1}^k X_i \right)$. \square

Lemma 3.18. *There exists T -cyclic subspaces M_1, \dots, M_s such that $W = \bigoplus_{i=1}^s M_i$.*

Proof. We proceed by induction on $k = \dim W$. The claim is vacuously true for $k = 0$. Assume the claim holds true for $k \leq n$, then for $k = n + 1$, let $W' = \text{im } q(T) \subseteq W$. Let $T' = T_{W'}$, then $f_{T'}(t) \mid f_T(t)$ since $f_{T'}(t) = q(t)^d$. Therefore we can apply our hypothesis to T' and W' .

Let $W' = \bigoplus_{i=1}^{s'} M'_i$ where M'_i is T' -cyclic thus T -cyclic. Suppose M'_i is generated by $x'_i \in M'_i$, since $x'_i \in \text{im } q(T)$, there exists x_i such that $q(T)x_i = x'_i$. Let M_i be the T -cyclic subspace generated by x_i for $i = 1, \dots, s'$. Clearly if $M'_i \subseteq M_i$. We claim that

$$\dim M_i = \dim M'_i + \deg q(t) \quad (21)$$

In fact, this is just rank-nullity theorem, since $\dim \ker M_i = \deg q(t)$. Let $Z' = Z \cap W' = \ker q(T_{W'})$. By Lemma 3.16,

$$Z' = \bigoplus_{i=1}^s (Z \cap M_i) = \bigoplus_{i=1}^s (Z \cap M'_i) \quad (22)$$

Also, $\dim Z' = \sum_{i=1}^s \dim (Z \cap M_i) = s \deg q(t)$.

We then use Lemma 3.17 to obtain T -cyclic subspaces $M_{s'+1}, \dots, M_s$, with $M_i \in Z$, such that $Z = Z' \oplus \left(\bigoplus_{i=s'+1}^s M_i \right)$. Finally we claim $W = \bigoplus_{i=1}^s M_i$. By Lemma 3.16, we only need to check if $\dim W$ and $\ker q(T)$ satisfy corresponding relations. We have

$$\begin{aligned} \bigoplus_{i=1}^s (Z \cap M_i) &= \left(\bigoplus_{i=1}^{s'} (Z \cap M_i) \right) \oplus \left(\bigoplus_{i=s'+1}^s (Z \cap M_i) \right) \\ &= Z' \oplus \left(\bigoplus_{i=s'+1}^s M_i \right) = Z \end{aligned} \quad (23)$$

where the second-last equality follows from $M_i \subseteq Z$ for $i = s' + 1, \dots, s$. On the other hand, by (21)

$$\begin{aligned} \dim W &= \sum_{i=1}^s \dim M_i = \sum_{i=1}^{s'} \dim M'_i + s' \deg q(t) + \sum_{i=s'+1}^s \dim M_i \\ &= \sum_{i=1}^{s'} \dim M'_i + s' \deg q(t) + (s - s') \deg q(t) = \sum_{i=1}^{s'} \dim M'_i + s \deg q(t) \end{aligned} \quad (24)$$

Notice $\bigoplus_{i=1}^{s'} M'_i = W' = \text{im } q(T)$ and $\dim \ker M_i = \deg q(T)$, (24) is

$$\dim W = \sum_{i=1}^{s'} \dim M'_i + s \deg q(t) = \dim \text{im } q(T) + \dim \ker q(T) = k \quad (25)$$

by the rank-nullity theorem. Hence the claim holds true for $\dim W = k$ as well. By induction, the claim holds for all k , and we are done. \square

Remark. The T -cyclic subspace generated by x is indeed the smallest T -invariant subspace in V , and therefore cannot be decomposed further.

Having Lemma 3.18, we successfully established a method decomposing V into as many T -invariant subspaces as possible, combine this result with the Primary Decomposition Theorem, we have reached our ultimate goal, as demonstrated by the next two theorems.

Theorem 3.19. *Let V be a finite dimensional vector space, $T \in \mathcal{L}(V)$. There exist T -cyclic subspaces M_1, \dots, M_s such that*

- $V = \bigoplus_{i=1}^s M_i$
- $f_{T_{M_i}}(t)$ is a power of irreducible polynomial over $\mathbb{F}[t]$.
- For any such decomposition, the number of polynomials such that $f_{T_{M_i}}(t) = q(t)^p$ is

$$\frac{2 \text{Nullity}(q(T)^p) - \text{Nullity}(q(T)^{p+1}) - \text{Nullity}(q(T)^{p-1})}{\deg q(t)} \quad (\star)$$

Proof. Let $f_T(t) = \prod_{i=1}^k q_i(t)^{d_i}$, then we can generate M_i as the following. First decompose V into primary subspaces using the Primary Decomposition Theorem. For each of the primary subspace, use Lemma 3.18 to decompose it into T -cyclic subspaces. The minimality of cyclic subspaces guarantee a maximal decomposition, and therefore $V = \bigoplus_{i=1}^s M_i$. Since $f_{T_{M_i}}(t) \mid f_{W_j}(t) = q_j(t)^{d_j}$, where W_j is the corresponding primary subspace of V , $f_{T_{M_i}}(t)$ is a power of irreducible polynomial, as desired.

To prove the huge formula, let $\phi(T, q(t), p)$ be the number of polynomials such that $f_{T_{M_i}}(t) = q(t)^p$, it suffices to show that

$$\phi(T, q(t), p) = \frac{2 \text{Nullity}(q(T)^p) - \text{Nullity}(q(T)^{p+1}) - \text{Nullity}(q(T)^{p-1})}{\deg q(t)} \quad (26)$$

It looks just like the Navier-Stokes Equation, $\rho \frac{Dv}{Dt} = -\nabla p + \nabla \cdot \mathbb{T} + \rho f$, but it is much easier to solve. In fact, if we restrict T on M_i , clearly we have

$$\phi(T_{M_i}, q(t), p) = \begin{cases} 1 & \text{if } f_{T_{M_i}}(t) = q(t)^p \\ 0 & \text{otherwise} \end{cases} \quad (27)$$

We show this is equal to (\star) restricted to T_{M_i} . First consider if $f_{T_{M_i}}(t) = q(t)^p$. Since $\text{Nullity}(q(T_{M_i})^p) = \dim M_i$ by the Cayley-Hamilton Theorem, and $\text{Nullity}(q(T_{M_i})^{p-1}) = \dim \text{im } q(T_{M_i}) = \dim M'_i$

$$\begin{aligned} \phi(T_{M_i}, q(t), p) &= 1 = \frac{\dim M_i - \dim M'_i}{\deg q(T)} \\ &= \frac{2 \dim M_i - \dim M_i - \dim M'_i}{\deg q(T)} \\ &= \frac{2 \text{Nullity}(q(T_{M_i})^p) - \text{Nullity}(q(T_{M_i})^{p+1}) - \text{Nullity}(q(T_{M_i})^{p-1})}{\deg q(t)} \end{aligned} \quad (28)$$

On the other hand, if $f_{T_{M_i}}(t) \neq q(t)^p$, then there exists some $a \neq p$ such that $q(T)^a$ annihilates M_i . If $a \leq p-1$, we have $\text{Nullity}(q(T_{M_i})^p) = \text{Nullity}(q(T_{M_i})^{p-1}) = \dim M_i$, and (\star) restricted to T_{M_i} evaluate to 0. If $a \geq p+1$, then

$$\text{Nullity}(q(T_{M_i})^{p+1}) - \text{Nullity}(q(T_{M_i})^p) = \text{Nullity}(q(T_{M_i})^p) - \text{Nullity}(q(T_{M_i})^{p-1}) = \deg q(t) \quad (29)$$

(\star) restricted to T_{M_i} evaluate to 0 as well. Hence in both cases our claim holds true. Therefore,

$$\begin{aligned}
\phi(T, q(t), p) &= \sum_{i=1}^s \phi(T_{M_i}, q(t), p) \\
&= \frac{1}{\deg q(t)} \sum_{i=1}^s 2 \text{Nullity}(q(T_{M_i})^p) - \text{Nullity}(q(T_{M_i})^{p+1}) - \text{Nullity}(q(T_{M_i})^{p-1}) \\
&= \frac{2 \text{Nullity}(q(T)^p) - \text{Nullity}(q(T)^{p+1}) - \text{Nullity}(q(T)^{p-1})}{\deg q(t)}
\end{aligned} \tag{30}$$

since $\sum_{i=1}^s \text{Nullity}(q(T_{M_i})^p) = \text{Nullity}(q(T)^p)$. \square

Remark. Note that the Navier-Stocks equation is used nowhere in the proof.

Remark. Please check this proof, especially the dimensions. I might have messed up on some dimensions of kernel and images.

The previous theorem has finished our objective of decomposition, and by Proposition 3.10, we can put T into block-diagonal matrix form. The following is its formal description.

Theorem 3.20 (Rational Canonical Form). *Let V be a finite dimensional vector space over \mathbb{F} , $L \in \mathcal{L}(V)$. There exists a basis β such that $[T]_\beta$ is block-diagonal and each block is the companion matrix of a power of $q(t)$, a irreducible polynomial over $\mathbb{F}[t]$.*

Moreover any two of the bases with the property will give equivalent matrices; that is, two matrices with same block-diagonal entries in different orders.

Such β is called a rational canonical basis, and $[T]_\beta$ is a rational canonical form.

Proof. Most parts of the proof follow from Theorem 3.19. It only remains to choose β . This is quite easy as well. Let $V = \bigoplus_{i=1}^s M_i$, with each M_i cyclic. Let $\beta_i = \{x_i, Tx_i, \dots, T^{\dim M_i - 1} x_i\}$ be the basis for M_i . By Proposition 3.2, each $[T_{M_i}]_{\beta_i}$ is a companion matrix. By Theorem 3.19, $f_{T_{M_i}}(t)$ is a power of some irreducible polynomial over $\mathbb{F}[t]$. By Proposition 3.10, $[T]_\beta$ is block diagonal, where $\beta = \bigcup_{i=1}^s \beta_i$. \square

Remark. Some texts define the rational canonical form to be with the least companion matrices on its diagonal instead. It turns out both ways have advantages, depending on what we are working with. For the least companion matrices decomposition, it does not matter which field we are working in, and eventually the rational canonical form will all look the same. In our case, the rational canonical form is much easier for computational purposes instead.

3.4 Jordan Canonical Form

In last section we see how we can decompose a matrix into block-diagonal form. Although the rational canonical form seems good enough, it has a serious issue; that is, it has non-zero entries below the diagonal as well, which makes the world you and I live in more complicated than ever before. It is empirically helpful to make the blocks upper-triangular. However, the question is, can we actually put the matrix into block-diagonal form so that every block has no entry below the diagonal?

“The answer is yes, but no.”

—Kevin Purbhoo⁴, 2015

Aside from that, the answer is yes if $f_T(t)$ splits over $\mathbb{F}[t]$. When we are able to do so, the resultant matrix is called a Jordan Canonical Form, and the following is its formal description.

⁴Kevin Purbhoo is a professor in the Department of Combinatorics and Optimization, University of Waterloo.

Theorem 3.21 (Jordan Canonical Form). *Let V be a finite dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$. If $f_T(t)$ splits, then there exists a basis β for V , such that $[T]_\beta$ is block-diagonal, and every diagonal block is a Jordan block $J_\lambda^n \in M_{n \times n}(\mathbb{F})$, i.e.*

$$J_\lambda^n = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & \lambda \end{pmatrix}$$

A matrix in such form is called a Jordan Canonical Form. Any two Jordan Canonical Forms for T are equivalent. The basis β is called a Jordan Canonical Basis, and this basis is not unique.

Proof. Since $f_T(t)$ splits, we can write V as a direct sum of generalized λ -eigenspaces, i.e. $V = \bigoplus_{\lambda} K_\lambda$. By Theorem 3.20, we can write V as a direct sum of T -cyclic subspaces as well. Let M_i be one of the T -cyclic subspaces, generated by $x_i \in V$. It follows that $M_i \subseteq K_\lambda$ for some eigenvalue λ . Let $\dim W = p$. Consider the following cycle of generalized eigenvectors:

$$\delta_i = \{(T - \lambda I)^{p-1}x_i, (T - \lambda I)^{p-2}x_i, \dots, (T - \lambda I)x_i, x_i\} \quad (31)$$

We claim that δ_i is a basis for M_i . It suffices to check the linear independency of δ_i . In fact, if there exists a non-trivial linear combination

$$\sum_{j=1}^p a_j (T - \lambda I)^{j-1} x_i = 0 \quad (32)$$

We can set $g(t) = \sum_{j=1}^p a_j (t - \lambda)^{j-1}$. Clearly $\deg g(t) < p$ and we can write $g(t) = \sum_{j=1}^p a'_j t^{j-1}$, and $g(T)x_i = 0$.

However, by Proposition 3.2, since $\{x_i, Tx_i, \dots, T^{p-1}x_i\}$ is a basis for M_i , there cannot exist a polynomial $f(t)$ with degree less than p that annihilates x_i , contradiction. (Here we still need to check if $a'_j \neq 0$ for some j , but that is pretty obvious. Let j_{\max} be the largest index such that $a_j \neq 0$, then $a'_{j_{\max}} \neq 0$ as well). Hence δ_i is linearly independent and a basis for M_i .

Next we compute $[T_{M_i}]_{\delta_i}$,

$$\begin{aligned} T((T - \lambda I)^{p-1}x_i) &= (T - \lambda I + \lambda I)((T - \lambda I)^{p-1}x_i) \\ &= (T - \lambda I)^p x_i + \lambda I((T - \lambda I)^{p-1}x_i) = \lambda(T - \lambda I)^{p-1}x_i \end{aligned} \quad (33)$$

and

$$\begin{aligned} T((T - \lambda I)^j x_i) &= (T - \lambda I + \lambda I)((T - \lambda I)^j x_i) \\ &= (T - \lambda I)^{j+1} x_i + \lambda(T - \lambda I)^j x_i \end{aligned} \quad (34)$$

for $0 \leq j < p-1$, hence

$$[T_{M_i}]_{\delta_i} = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix} \quad (35)$$

is a Jordan block indeed. If we take $\delta = \bigcup_{i=1}^s \delta_i$, our resultant matrix $[T]_\delta$ is block-diagonal with each diagonal block a Jordan block, as desired. \square

This form has millions of applications to it, and is essential in linear algebra. We can read off the characteristic polynomial, the determinant, the trace directly from a Jordan Canonical Form. Less obviously we can read off the minimal polynomial, by taking the least common multiple of the minimal polynomial of each Jordan block (See Lemma 3.14). Moreover the dimension of λ -eigenspace is precisely the number of Jordan blocks with λ on its diagonal.

From the basis we can determine easily a basis for each eigenspace, kernel and image of T . Also we can compute the powers of T and $\exp(T)$ efficiently⁵.

Theoretically, we have the following general strategy of proof.

HAMMER 3.22. *To prove a statement, we can first prove the statement for Jordan blocks, then deduce the general case.*

Remark. The above statement is really a **HAMMER**.

To illustrate this, we shall prove Lemma 1.8 and 1.9, which were never proven before. Recall that $S = \{\lambda \in \mathbb{C} \mid |\lambda| < 1\} \cup \{1\}$.

Lemma 3.23. *Let $A \in M_{n \times n}(\mathbb{C})$. $\lim_{m \rightarrow \infty} A^m$ exists if and only if every eigenvalue of A belongs to S , and if 1 is an eigenvalue, then $\dim E_\lambda = \text{mult}(\lambda)$.*

Proof. By the fundamental theorem of algebra, $f_A(t)$ splits over \mathbb{C} . Therefore we can write A in Jordan Canonical Form, i.e. $A = QJQ^{-1}$. So $\lim_{m \rightarrow \infty} A^m = \lim_{m \rightarrow \infty} QJ^mQ^{-1}$. It suffices to show that every Jordan block commits a limit. We show by induction on m that, for $J \in M_{n \times n}(\mathbb{C})$,

$$(J_\lambda^m)_{ij} = \begin{cases} \binom{m}{j-i} \lambda^{m-j+i} & \text{if } j \geq i \\ 0 & \text{if } j < i \end{cases} \quad (36)$$

The case $m = 1$ is obvious, so is the case when $j < i$. Assume the claim holds true for $m = k$, then for $m = k + 1$,

$$\begin{aligned} (J_\lambda^{k+1})_{ij} &= (J_\lambda^k J_\lambda)_{ij} = (J_\lambda^k)_{i, (j-1)} + \lambda (J_\lambda^k)_{ij} \\ &= \binom{k}{j-1-i} \lambda^{k+1-j-i} + \binom{k}{j-i} \lambda^{k+1-j-i} \\ &= \left(\binom{k}{j-1-i} + \binom{k}{j-i} \right) \lambda^{k+1-j-i} \\ &= \binom{k+1}{j-i} \lambda^{k+1-j-i} \end{aligned} \quad (37)$$

as desired. Hence by induction, the claim holds true for all m .

Next we show that $\lim_{m \rightarrow \infty} J_\lambda^m$ exists if $\lambda \in S \setminus \{1\}$. Clearly for fixed $l = j - i$, the exponential term dominates the binomial coefficient, which is a polynomial, and hence the limit is 0⁶. If $\lambda = 1$, when $n = 1$ it clearly converges, otherwise we have $(J_1^m)_{12} = m$ which does not converge as $m \rightarrow \infty$. So if 1 is an eigenvalue of J , $\dim E_1 = 1 = \text{mult}(1)$, as desired. When $\lambda \notin S$, basic calculus shows that the limit does not exist. Hence $\lim_{m \rightarrow \infty} J_\lambda^m$ exists if and only if $\lambda \in S$, and if $\lambda = 1$, $\dim E_1 = 1 = \text{mult}(1)$. Thus we have shown that the limit exists under the same condition, by **HAMMER**, the claim holds for all A as well. \square

Remark. In class Purbhoo also shows that the second statement is equivalent to its Jordan counterpart, which is quite redundant.

Lemma 3.24. *Let $A \in M_{n \times n}(\mathbb{F})$, λ an eigenvalue of A . Then $\text{mult}(\lambda) > \dim E_\lambda$ if and only if there exist non-zero vectors $x, y \in \mathbb{F}_{col}^n$ such that $Ax = \lambda x$ and $Ay = \lambda y + x$.*

We shall prove a stronger result of this lemma.

⁵See assignment 1 for more details

⁶This is not a calculus class so we take this as granted.

Theorem 3.25. *Following the definitions of Lemma 3.24, the following are equivalent:*

- i) $\dim E_\lambda < \text{mult}(\lambda)$
- ii) $E_\lambda \neq K_\lambda$
- iii) $(t - \lambda)^2 \mid m_A(t)$
- iv) *There exist non-zero vectors $x, y \in \mathbb{F}_{col}^n$ such that $Ax = \lambda x$ and $Ay = \lambda y + x$.*
- v) $E_\lambda \cap \text{Col}(A - \lambda I) \neq \{0\}$

Proof. i) \iff ii) is obvious since $E_\lambda \subset K_\lambda$ and $\dim K_\lambda = \text{mult}(\lambda)$.

ii) \iff iii). Assume $E_\lambda \neq K_\lambda$, then there exists $x \in K_\lambda$ such that $(A - \lambda I)x \neq 0$. Thus $m_{T_{K_\lambda}}(t) \neq t - \lambda$. Hence $(t - \lambda)^2 \mid m_{T_{K_\lambda}}(t) \implies (t - \lambda)^2 \mid m_T(t)$.

iii) \implies iv). Assume $E_\lambda \neq K_\lambda$. Let $x_0 \in K_\lambda \setminus E_\lambda$. Let p be the smallest integer such that $(A - \lambda I)^p x_0 = 0$. From iii), $p \geq 2$. Set $y = (A - \lambda I)^{p-2} x_0$ and $x = (A - \lambda I)^{p-1} x_0$. Clearly $x, y \neq 0$, and it can be easily verified that $Ax = \lambda x$ and $Ay = \lambda y + x$.

iv) \implies ii). Assume $Ax = \lambda x$, $Ay = \lambda y + x$. Since $x \neq 0$, $y \notin E_\lambda$. But

$$(A - \lambda I)^2 y = (A - \lambda I)(Ay - \lambda y) = (A - \lambda I)x = 0 \quad (38)$$

Hence $y \in K_\lambda$, and $K_\lambda \neq E_\lambda$.

iv) \iff v). We have

$$(Ax = \lambda x \wedge Ay = \lambda y + x) \iff (x \in E_\lambda \wedge x = (A - \lambda I)y) \iff x \in (E_\lambda \cap \text{Col}(A - \lambda I)) \quad (39)$$

The proof is then complete. \square

Next and last application of the **HAMMER** is a criterion of similar matrices.

Theorem 3.26. *Let $A, B \in M_{n \times n}(\mathbb{F})$, then A is similar to B , i.e. there exists an invertible matrix $Q \in M_{n \times n}(\mathbb{F})$ such that $A = QBQ^{-1}$, if and only if for any polynomial $p(t) \in \mathbb{F}[t]$, $\text{rank}(p(A)) = \text{rank}(p(B))$.*

Proof. Assume first that A and B are similar, then for any $p(t) \in \mathbb{F}[t]$, $\text{rank}(p(A)) = \text{rank}(p(QBQ^{-1})) = \text{rank}(p(B))$ since multiplying by an invertible matrix preserves the rank.

On the other hand, recall (\star) from Theorem 3.19. The number of blocks with characteristic polynomial $f(t) = q(t)^d$ in a Rational Canonical Form only involves the nullity of $q(T)$. So A and B have the same number of them. Taking all such $q(t)$, we see that A and B has the same Rational Canonical Form. Hence they are similar. \square

Corollary 3.27. *A is similar to A^T . This is totally not obvious.*

Remark. Notice in the above proof, **HAMMER** does not even appear at all. Nevertheless, **HAMMER** is still a **HAMMER**.

4 Bilinear Forms and Orthogonal Diagonalization

4.1 Inner Product Space

Definition 4.1 (Bilinear Function). *Let V_1, V_2, V_3 be vector spaces over \mathbb{F} , then $f : V_1 \times V_2 \rightarrow V_3$ is **bilinear** if f is linear in V_1 and V_2 ; that is,*

$$\begin{aligned} f(x + kx', y) &= f(x, y) + kf(x', y) \\ f(x, y + ky') &= f(x, y) + kf(x, y') \end{aligned}$$

for $x, x' \in V_1, y, y' \in V_2, k \in \mathbb{F}$.

Example. Matrix multiplication is bilinear. In particular, if $V_1 = M_{k \times l}(\mathbb{F})$, $V_2 = M_{l \times m}(\mathbb{F})$ and $V_3 = M_{k \times m}(\mathbb{F})$, then $f : V_1 \times V_2 \rightarrow V_3$ given by $f(M_1, M_2) = M_1 M_2$ for $M_1 \in V_1, M_2 \in V_2$ is bilinear.

Example. Polynomial Multiplication is bilinear. In particular, if $V_1 = V_2 = V_3 = \mathbb{F}[t]$, then $m : V_1 \times V_2 \rightarrow V_3$ given by $m(f_1, f_2) = f_1 f_2$ for $f_1, f_2 \in \mathbb{F}[t]$ is bilinear.

However these are not of our interests. We introduce bilinear forms which we will be focusing on for the rest of the chapter.

Definition 4.2 (Bilinear Form). *Let V be a vector space over \mathbb{F} . A bilinear function $f : V \times V \rightarrow \mathbb{F}$ is called a **bilinear form**.*

Example. Let $V_1 = V_2 = \mathbb{R}^n$. If $x = (x_1, \dots, x_n)^t$ and $y = (y_1, \dots, y_n)^t$, then the map $\cdot : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ given by $x \cdot y = \sum_{i=1}^n x_i y_i$ is a bilinear form. This map is called the dot product, or the standard inner product if \mathbb{F} is a field over \mathbb{R} .

The dot product is used frequently in vector spaces over \mathbb{R} . We can measure the length of a vector and angle between two vectors using the dot product.

In fact, let $x \in \mathbb{R}^n$, then the length of x is $|x| = \sqrt{x \cdot x} = \sqrt{\sum_{i=1}^n x_i^2}$. The angle between two vectors are a little more complicated. Let $x, y \in \mathbb{R}^n$, then the angle between x and y , say θ , is given by $\cos \theta = \frac{x \cdot y}{|x| |y|}$. To verify the formula, we use the cosine law⁷,

$$\begin{aligned} \cos \theta &= \frac{|x|^2 + |y|^2 - |x - y|^2}{2|x||y|} = \frac{|x|^2 + |y|^2 - (|x|^2 - 2x \cdot y + |y|^2)}{2|x||y|} \\ &= \frac{x \cdot y}{|x||y|} \end{aligned} \tag{1}$$

However, if V is a vector space over \mathbb{C} , the idea of dot product would not make sense anymore, since, for example, the length of a vector could be a complex-valued number. The alternative in \mathbb{C} , as it turns out, is to use the complex conjugate. Let $V = \mathbb{C}^n$, consider the function $\cdot : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$ given by $x \cdot \bar{y} = \sum_{i=1}^n x_i \bar{y}_i$ for $x, y \in \mathbb{C}^n$. Now this function satisfies our demand. Since we can represent the length of x with a proper real number. In fact, if $x = (a_1 + b_1 i, \dots, a_n + b_n i)^t$, then $|x| = \sqrt{x \cdot \bar{x}} = \sqrt{\sum_{i=1}^n (a_i^2 + b_i^2)}$ which is properly defined for any x . We can then define angle in a similar manner, but more importantly, angle in the complex number case tells us more than angles in the real case. This is not intuitive. I do not know why.

If we look at our map above more carefully, we find that this map is actually not quite bilinear because it is not linear in y . Instead of trying to make it bilinear, we introduce the following terminology in the complex case.

⁷This is a linear algebra course, so we take this as granted

Definition 4.3 (Sesquilinear Form). Let V be a vector space over \mathbb{C} . A map $V \times V \rightarrow \mathbb{C}$ is called a **sesquilinear form** if it has the following properties

$$\begin{aligned} f(x + kx', y) &= f(x, y) + kf(x', y) \\ f(x, y + ky') &= f(x, y) + \bar{k}f(x, y') \end{aligned}$$

Remark. Notice that if $\Im(k) = 0$, then the above properties coincide with those of a bilinear form.

Example. The dot product defined above is a sesquilinear form, as one can verify.

For the rest of the section, we restrict our interests to \mathbb{R} and \mathbb{C} .

Definition 4.4 (Inner Product). Let V be a vector space over \mathbb{F} . An **inner product** on V is a function assigned to each ordered pair $(x, y) \in V \times V$ a scalar $\langle x, y \rangle \in \mathbb{F}$ with the following properties

1. The map $V \times V \rightarrow \mathbb{F}$ given by $(x, y) \rightarrow \langle x, y \rangle$ is bilinear if $\mathbb{F} = \mathbb{R}$, or sesquilinear if $\mathbb{F} = \mathbb{C}$.
2. The map is symmetric if $\mathbb{F} = \mathbb{R}$; that is, $\langle x, y \rangle = \langle y, x \rangle$, or Hermitian if $\mathbb{F} = \mathbb{C}$; that is, $\langle x, y \rangle = \overline{\langle y, x \rangle}$.
3. The map is positive definite; that is, $\langle x, x \rangle > 0$ for all $x \neq 0 \in V$.

Example. In \mathbb{R}^n , the map $\langle x, y \rangle = x \cdot y$ is an inner product. In \mathbb{C}^n , the map $\langle x, y \rangle = x \cdot \bar{y}$ is an inner product.

Example. If $V = C[0, 2\pi]$, the map $\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(t)g(t)dt$ is an inner product.

Definition 4.5 (Inner Product Space). An **inner product space** is a vector space endowed with a specific inner product $\langle \cdot, \cdot \rangle$.

Example. If V is an inner product space, then so is any $W \subset V$ by restricting the inner product to W .

Proposition 4.6. Let $A \in M_{m \times n}(\mathbb{F})$. The matrix $A^* \in M_{n \times m}(\mathbb{F})$ given by $(A^*)_{ij} = \overline{A_{ji}}$ is called the **Hermitian adjoint** (of A). If $\mathbb{F} = \mathbb{C}$, it is also called the **conjugate transpose** of A . The $M_{m \times n}(\mathbb{F})$ is an inner product space with $\langle A, B \rangle = \text{tr}(AB^*)$.

We have, if $\langle \cdot, \cdot \rangle_{\mathbb{F}^n}$ is the standard inner product in \mathbb{F}^n , then

$$\langle Ax, y \rangle_{\mathbb{F}^m} = \langle x, A^*y \rangle_{\mathbb{F}^n} \quad (\star)$$

for $x \in \mathbb{F}^n$ and $y \in \mathbb{F}^m$.

Proof. To check $\langle A, B \rangle = \text{tr}(AB^*)$, we need to check that it satisfies the 3 rules. First of all, we have $\langle A + kA', B \rangle = \text{tr}((A + kA')B^*) = \text{tr}(AB^*) + k \text{tr}(A'B^*)$, so this map is linear in A . Also, $\langle A, B + kB' \rangle = \text{tr}(A(B + kB')^*) = \text{tr}(AB^*) + \bar{k} \text{tr}(AB'^*)$. Hence this map is sesquilinear.

To check symmetry, we have $\text{tr}(AB^*) = \text{tr}(A^*B)$ by the property of trace. I mean, yeah, you can assume it's true because the trace is not discussed in class. To check positive definiteness, we have $\text{tr}(AA^*) > 0$ for $A \neq 0$, since each diagonal entry of the product is the standard inner product in \mathbb{C}^n , which is 0 if and only if every column vector is 0, i.e. $A = 0$. Hence $\langle A, B \rangle = \text{tr}(AB^*)$ is a well-defined inner product.

To show that (\star) holds, we use the following well-known identity on inner products, which asserts $\langle u, v \rangle = u^t \bar{v} = v^* u$. Then

$$\langle Ax, y \rangle = (Ax)^t \bar{y} = x^t A^t \bar{y} = x^t \overline{A^* y} = \langle x, A^* y \rangle \quad (2)$$

as desired. Hence our formula is true. \square

The following are some useful properties of an inner product space.

Proposition 4.7. If V is an inner product space, then

1. $\langle a, 0 \rangle = \langle 0, a \rangle = 0$ for all $a \in V$.
2. $\langle x, x \rangle = 0 \iff x = 0$.

$$3. \langle x, y \rangle = \langle x, z \rangle \forall x \in V \iff y = z.$$

Proof. 1 follows directly from sesquilinearity, 2 follows from positive definiteness and 1. To see 3, consider $x = y - z$, then $\langle y - z, y - z \rangle = 0 \iff y = z$. \square

Remark. A bilinear map satisfying property 3 is said to be non-degenerate. It is interesting and worth to study bilinear map, instead of sesquilinear map, that is non-degenerate over \mathbb{C} . Notice here, positive definiteness implies non-degeneracy, but not the other way around.

Finally we formally define length in an inner product space.

Definition 4.8 (Norm of a Vector). *Let V be an inner product space. For a vector $x \in V$, the **norm**, or the **length** of x is $\|x\| = \sqrt{\langle x, x \rangle}$.*

Example. If $V = \mathbb{F}^n$ with the standard inner product, then $\|x\|$ is the Euclidean length.

The following are the key properties of length.

Theorem 4.9. *Let V be an inner product space, $x, y \in V$, then*

1. $\|cx\| = |c| \|x\|$.
2. $\|x\| \geq 0$ and $\|x\| = 0 \iff x = 0$.
3. (Cauchy-Schwarz Inequality) $|\langle x, y \rangle| \leq \|x\| \|y\|$.
4. (Triangle Inequality) $\|x + y\| \leq \|x\| + \|y\|$.

Proof. 1 and 2 are easy and straightforward. For 3, we have

$$0 \leq \|x - cy\|^2 = \langle x - cy, x - cy \rangle = \langle x, x \rangle - \bar{c}\langle x, y \rangle - c\langle y, x \rangle + c\bar{c}\langle y, y \rangle \quad (3)$$

Substitute $c = \frac{\langle x, y \rangle}{\langle y, y \rangle}$, (3) becomes

$$\begin{aligned} 0 &\leq \langle x, x \rangle - \frac{\overline{\langle x, y \rangle} \langle x, y \rangle}{\langle y, y \rangle} - \frac{\langle x, y \rangle \langle y, x \rangle}{\langle y, y \rangle} + \frac{\langle x, y \rangle \overline{\langle x, y \rangle}}{\langle y, y \rangle} \\ &= \langle x, x \rangle - \frac{\overline{\langle x, y \rangle} \langle x, y \rangle}{\langle y, y \rangle} \iff \overline{\langle x, y \rangle} \langle x, y \rangle \leq \|x\|^2 \|y\|^2 \\ &\implies |\langle x, y \rangle|^2 \leq \|x\|^2 \|y\|^2 \implies |\langle x, y \rangle| \leq \|x\| \|y\| \end{aligned} \quad (4)$$

For 4, we have

$$\begin{aligned} \|x + y\|^2 &= \langle x + y, x + y \rangle \\ &= \langle x, x \rangle + 2\Re\langle x, y \rangle + \langle y, y \rangle \\ &\leq \langle x, x \rangle + 2|\langle x, y \rangle| + \langle y, y \rangle \\ &\leq \|x\|^2 + 2\|x\| \|y\| + \|y\|^2 \text{ (C-S Inequality)} \\ &= (\|x\| + \|y\|)^2 \end{aligned} \quad (5)$$

Taking the square root gives the inequality. \square

Remark. The Cauchy-Schwarz inequality is sometimes called Cauchy-Schwarz-Bunyakovsky⁸-I-Can't-Spell-It inequality.

⁸I can't spell this either. This is due to Wikipedia.

4.2 Orthogonality

What we have seen in the last section is mostly useless without talking about orthogonality⁹.

Definition 4.10 (Orthogonality and Orthonormal Basis). *Let V be an inner product space, we say $x, y \in V$ are **orthogonal** if $\langle x, y \rangle = 0$. A subset S of V is **orthogonal** if $\langle x, y \rangle = 0$ for all $x, y \in S$ and $x \neq y$.*

*x is called a unit vector if $\langle x, x \rangle = 1$. S is **orthonormal** if S is orthogonal and every vector in S is a unit vector. Moreover it is an **orthonormal basis** if S is a basis for V .*

Example. Recall in \mathbb{R}^n , $\langle x, y \rangle = 0$ if and if they are perpendicular to each other.

Example. If $x \neq 0$, then $\frac{x}{\|x\|}$ is a unit vector. This is used in normalization of a vector.

Remark. When working with inner product spaces, orthonormal bases are always preferable because they make WHOLE BUNCH OF THINGS WHOLE A LOT EASY.

Remark. All the definitions above would make sense even if $\langle \cdot, \cdot \rangle$ is not positive-definite.

Intuitively, one should think this as in \mathbb{R}^n when two vectors are at right angles to each other; however, this is not always the case in \mathbb{C}^n . Vectors 1 and i are at right angle to each other, but $\langle 1, i \rangle = -i$ is certainly not 0.

Definition 4.11 (Orthogonal Complement). *Let V be an inner product space. Let S and S' be subsets of V . We say S and S' are **orthogonal** if $\langle x, y \rangle = 0$ for all $x \in S$ and $y \in S'$, and we write $S \perp S'$.*

*Let S be a subset of V . The **orthogonal complement** of S is the set of all vectors x such that $\langle x, s \rangle = 0$ for all $s \in S$, denoted as*

$$S^\perp = \{y \in V \mid \langle y, x \rangle = 0 \forall x \in S\}$$

We will see why orthogonality and orthogonal sets are important in the rest of the section.

Proposition 4.12. *Every orthonormal set is linearly independent.*

Proof. Let $S = \{v_1, \dots, v_n\}$ be an orthonormal set, suppose we have a linear combination

$$\sum_{i=1}^n a_i v_i = 0 \tag{6}$$

for some $a_i \in \mathbb{F}$, then for $j = 1 \dots n$, we can apply $\langle \cdot, v_j \rangle$ on both sides. Since S is orthonormal,

$$\langle 0, v_j \rangle = \left\langle \sum_{i=1}^n a_i v_i, v_j \right\rangle = \sum_{i=1}^n a_i \langle v_i, v_j \rangle = a_j \langle v_j, v_j \rangle = a_j \tag{7}$$

By Proposition 4.7, $a_j = 0$ for $j = 1 \dots n$. Hence such linear combination must be the trivial one, and therefore S is linearly independent. \square

Next we define the projection map. This will be essential.

Theorem 4.13 (Projection Formula a.k.a Baby). *Let V be an inner product space. Let W be a finite dimensional subspace of V . Suppose $\gamma = \{w_1, \dots, w_m\}$ is an orthonormal basis for W . Define $P_W \in \mathcal{L}(V)$ by*

$$P_W(y) = \sum_{i=1}^m \langle y, w_i \rangle w_i$$

Then $P_W(y) \in W$, and $y - P_W(y) \in W^\perp$ and $P_W(y)$ is the unique vector in W with this property. Moreover, $P_W(y)$ is the unique closest vector in W to y . In particular if $y \in W$ then $P_W(y) = y$.

*This map is called the **orthogonal projection operator** onto W .*

⁹I mean not totally, they are used to construct Hilbert Spaces.

Proof. Clearly $P_W(y) \in W$. To show that $y - P_W(y) \in W^\perp$, we have

$$\langle y - P_W(y), w_i \rangle = \langle y, w_i \rangle - \langle P_W(y), w_i \rangle = \langle y, w_i \rangle - \sum_{j=1}^m \langle y, w_j \rangle \langle w_i, w_j \rangle = \langle y, w_i \rangle - \langle y, w_i \rangle = 0 \quad (8)$$

for all $i = 1, \dots, m$. Therefore $y - P_W(y) \in W^\perp$. To show that this vector is unique. Suppose $w = \sum_{i=1}^m a_i w_i$ is some vector in W , then clearly $\langle y - P_W(y), w \rangle = 0$. Assume there exists some vector z such that $y - z \in W^\perp$, then

$$\langle y - z, w \rangle = 0 \implies \langle z, w \rangle = \langle y, w \rangle = \langle P_W(y), w \rangle \quad (9)$$

This is for all $w \in W$. Apply Proposition 4.7.3 to the inner product restricted to W , we see $z = P_W(y)$. Therefore this vector is unique.

To prove that the distance is the shortest is a pain in the ass. Let $w \in W$, then

$$\begin{aligned} \|y - w\|^2 &= \|y - P_W(y) + P_W(y) - w\|^2 \\ &= \langle y - P_W(y) + P_W(y) - w, y - P_W(y) + P_W(y) - w \rangle \\ &= \langle y - P_W(y), y - P_W(y) \rangle + \langle P_W(y) - w, P_W(y) - w \rangle \\ &\quad + \langle P_W(y) - w, y - P_W(y) \rangle + \langle y - P_W(y), P_W(y) - w \rangle \\ &= \|y - P_W(y)\|^2 + \|P_W(y) - w\|^2 \geq \|y - P_W(y)\|^2 \end{aligned} \quad (10)$$

since $y - P_W(y) \in W^\perp$ and $P_W(y) - w \in W$. Equality occurs if and only if $P_W(y) = w$. Therefore the distance between y and w is minimal when $P_W(y) = w$. \square

Remark. Note that we have not proven an orthogonal basis exists yet.

Remark. Intuitively one should think $P_W(y)$ depends on the choice of γ , but uniqueness guarantees it does not.

Remark. This definition of projection does not contradict the remark after Theorem 3.9. One can compute that indeed $P_W = P_W^2$.

With the above map in mind, we can construct an orthonormal basis starting from any basis $\gamma = \{w_1, \dots, w_m\}$. This is the famous cancerous Gram-Schmidt Process.

Starting from $v_1 = w_1$, generate v_k for $k = 2 \dots m$ as the following,

$$v_k = w_k - \sum_{i=1}^{k-1} \frac{\langle w_k, v_i \rangle}{\langle v_i, v_i \rangle} v_i \quad (11)$$

Then $\beta = \left\{ \frac{v_1}{\|v_1\|}, \dots, \frac{v_m}{\|v_m\|} \right\}$ is an orthonormal basis.

One shall notice that the change of basis formula in this case for γ and β looks like

$$\Psi_\gamma = \Psi_\beta R \quad (12)$$

for some R upper-triangular with positive diagonal entries, since (11) implies that

$$w_k = \|v_k\| \frac{v_k}{\|v_k\|} + \sum_{i=1}^{k-1} \langle w_k, v_i \rangle \frac{v_i}{\|v_i\|} \quad (13)$$

in which the first coefficient is the (positive) diagonal entry and the rest above diagonal.

The following theorem shows that the above process works.

Theorem 4.14. *Let β be a generated basis following the above process, then β is an orthonormal basis for V the unique ordered set that satisfy these properties.*

Proof. First we show that β is an orthonormal basis for V . Let $W_k = \text{Span}(w_1, \dots, w_k)$, we shall show by induction on k that $\left\{ \frac{v_1}{\|v_1\|}, \dots, \frac{v_k}{\|v_k\|} \right\}$ is an orthonormal basis for W_k .

For $k = 0$ this is trivial. Assume the claim holds true for $k = n - 1$, then for $k = n$, by hypothesis, (11) is equivalent to

$$v_n = w_n - P_{W_{n-1}}(w_n) \quad (14)$$

where $P_{W_{n-1}}(w_n)$ is the projection map defined in Theorem 4.13. Also by Theorem 4.13, $v_n \in W_{n-1}^\perp$. Since $W_n \not\subset W_{n-1}$, therefore $v_n \neq 0 \implies \frac{v_n}{\|v_n\|}$ is a unit vector. Moreover, for $i = 1, \dots, n - 1$,

$$v_n \in W_{n-1}^\perp \implies \left\langle \frac{v_k}{\|v_k\|}, \frac{v_i}{\|v_i\|} \right\rangle = 0 \quad (15)$$

Hence $\left\{ \frac{v_1}{\|v_1\|}, \dots, \frac{v_n}{\|v_n\|} \right\}$ is an orthonormal basis for W_n as desired. By induction, the claim holds for all k . In particular when $k = m$, we have $\beta = \left\{ \frac{v_1}{\|v_1\|}, \dots, \frac{v_m}{\|v_m\|} \right\}$ is an orthonormal basis for V . To show that this basis is also unique, assume there exists another basis $\beta' = \{v'_1, \dots, v'_m\}$ with property (11), that is

$$\Psi_\gamma = \Psi_{\beta'} R' \quad (16)$$

for some upper-triangular R' . Then we can write

$$\Psi_{\beta'} = \Psi_\gamma R'^{-1} \quad (17)$$

Denote $R'_{ii} = a_i > 0$, then $R'^{-1}_{ii} = a_i^{-1}$. Consider $\beta'' = \{a_1 v'_1, \dots, a_m v'_m\}$, then

$$\Psi_{\beta''} = \Psi_\gamma R_0 \quad (18)$$

where R_0 is upper-triangular with diagonal entries 1. Clearly $a_k v'_k = w_k - x_k$ for some $x_k \in W_{k-1}$. By a similar fashion, $\{v'_1, \dots, v'_k\}$ is a (orthonormal) basis for W_k , by Theorem 4.13, $x_k = P_{W_{k-1}}(w_k)$ since $a_k v'_k \in W_{k-1}^\perp$. This forces $a_k v'_k = v_k$. Since $a_k > 0$, $|a_k| = \|v'_k\| = 1$. Hence $v'_k = \frac{v_k}{\|v_k\|} \implies \beta' = \beta$. \square

Corollary 4.15. *Every finite-dimensional vector space has an orthonormal basis.*

Proof. Since every finite-dimension vector space has a basis, we can apply the Gram-Schmidt process and we obtain an orthonormal basis. \square

This is essential. In fact, there is a more general statement.

Theorem 4.16. *Let V be a finite-dimensional vector space over \mathbb{F} , $\langle \cdot, \cdot \rangle$ a symmetric form if $\mathbb{F} = \mathbb{R}$ or Hermitian form if $\mathbb{F} = \mathbb{C}$. There exists an orthonormal basis for V relative to $\langle \cdot, \cdot \rangle$ if and only if $\langle \cdot, \cdot \rangle$ is an inner product.*

Proof. One way is made clear by Corollary 4.15. It only suffices to show that if there exists an orthonormal basis for V , then $\langle \cdot, \cdot \rangle$ is an inner product.

Let $\beta = \{v_1, \dots, v_n\}$ be an orthonormal basis for V , clearly

$$\langle v_i, v_j \rangle = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} \quad (19)$$

Let $v \in V$ be a non-zero vector, i.e. $v = \sum_{i=1}^n a_i v_i$, then

$$\langle v, v \rangle = \left\langle \sum_{i=1}^n a_i v_i, \sum_{i=1}^n a_i v_i \right\rangle = \sum_{i=1}^n |a_i|^2 > 0 \quad (20)$$

therefore $\langle \cdot, \cdot \rangle$ is positive definite. Hence it is also an inner product. \square

Remark. In the theorem statement, a symmetric form is a bilinear form that is symmetric, and a Hermitian form is a sesquilinear form that is Hermitian.

What follows is many applications of the (cancerous) Gram-Schmidt process. Although we assumed an inner product space and a proper basis to start the process, we can also plug in so-called “bad” inputs.

Theorem 4.16 provides a tool for us to test if a symmetric (Hermitian) form is an inner product. Because if we pick a basis for V and apply Gram-Schmidt to it, the output will be an orthonormal basis if and only if the given form is an inner product. That is, if the given form is NOT an inner product, then Gram-Schmidt MUST reveal it. What can go wrong in this case is that the process will produce a vector v_k such that $\langle v_k, v_k \rangle \leq 0$ to contradict the positive definiteness of an inner product.

On the other hand, if the set of vectors input is not linearly independent, Gram-Schmidt will reveal it as well. In fact if w_k can be written as a linear combination of w_i for $i = 1, \dots, k-1$, then the output v_k will be 0 as a consequence. We can fix this by deleting w_k and carry on with the rest of the set. As long as the given set of vectors is linearly independent, Gram-Schmidt will produce an orthonormal basis of the span of them. Remember, the moral is, we can always reduce γ to an linearly independent set by deleting bad entries and run Gram-Schmidt with it.

Moreover, the validity of Gram-Schmidt process guarantees that the projection map is well-defined on any finite-dimensional W subspace of V . (Notice this is not the case for if $\dim W$ is not finite, insert counterexample). Following is a random proposition.

Proposition 4.17. *Let V be an inner product space over \mathbb{F} , $W_1, W_2 \subset V$ such that $W_1 \perp W_2$. Let P_{W_1} and P_{W_2} be the corresponding projection map, then $P_{W_1}P_{W_2} \equiv 0$.*

Proof. Let $x \in V$, $\gamma = \{v_1, \dots, v_n\}$ and $\beta = \{w_1, \dots, w_m\}$ be orthonormal bases for W_1 and W_2 respectively. We have

$$P_{W_1}P_{W_2}x = P_{W_1}\left(\sum_{i=1}^m \langle x, w_i \rangle w_i\right) = \sum_{i=1}^m \sum_{j=1}^n \langle \langle x, w_i \rangle w_i, v_j \rangle = 0 \quad (21)$$

□

Next we introduce some properties of orthogonal compliments.

Theorem 4.18. *Let V be a finite-dimensional vector space over \mathbb{F} , $W \subset V$. Then*

1. $(W^\perp)^\perp = W$
2. $V = W \oplus W^\perp$
3. $I_v = P_W + P_{W^\perp}$
4. $W = \text{im } P_W = \ker P_{W^\perp}$ and $W^\perp = \ker P_W = \text{im } P_{W^\perp}$

Proof. We shall prove this theorem in the natural order, so we start with 3. It suffices to show that for every $x \in V$,

$$(I_v - P_W)x = P_{W^\perp}x \quad (22)$$

which is equivalent to $(I_v - P_W)x \in W^\perp$ and $\langle x - (I_v - P_W)x, y \rangle = 0$ for $y \in W^\perp$ by Theorem Baby. The first condition is met since $(I_v - P_W)x = x - P_Wx \in W^\perp$ by Baby. The second condition is met since

$$\langle x - (I_v - P_W)x, y \rangle = \langle P_Wx, y \rangle = 0 \quad (23)$$

Hence the result.

To prove 4, certainly we have $W \subseteq \text{im } P_W$ by definition. Since $P_Ww = w$ for $w \in W$, $\text{im } P_W = W$, as desired. On the other hand,

$$y \in W \iff P_Wy = y \implies (I_v - P_{W^\perp})y = y \iff P_{W^\perp}y = 0 \implies y \in \ker P_{W^\perp} \quad (24)$$

and similarly for the other equality.

To prove 2, we have $\dim W + \dim W^\perp = \dim \operatorname{im} P_W + \dim \ker P_W = n$ from 4 and the rank-nullity theorem. From 3 we have $v = P_W v + P_{W^\perp} v$, and hence $V = W \oplus W^\perp$.

Lastly, from 3,

$$P_W + P_{W^\perp} = I_v \implies P_{W^\perp} + P_{(W^\perp)^\perp} = I_v \implies P_W = P_{(W^\perp)^\perp} \implies W = (W^\perp)^\perp \quad (25)$$

□

From this we can have more applications to the cancerous Gram-Schmidt process. We can find a basis for W^\perp knowing the previous theorem. In fact, if $\{w_1, \dots, w_m\}$ is a basis for W , we can extend it to a basis $\{w_1, \dots, w_m, v_1, \dots, v_n\}$ for V , and apply Gram-Schmidt to $\{v_1, \dots, v_n\}$, the result will be an orthonormal basis for W^\perp . If you don't believe this you can try it yourself, and we omit the proof.

The next application of the process is the Schur's Theorem.

Theorem 4.19 (Schur's Theorem). *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$. Suppose $f_T(t)$ splits, then there exists an orthonormal basis β such that $[T]_\beta$ is upper-triangular.*

Proof. If we have shown that for every linear operator T , there exists a basis γ such that $[T]_\gamma$ is upper-triangular we will be done since then we can apply Gram-Schmidt to γ to obtain an orthonormal basis β such that

$$\Psi_\gamma = \Psi_\beta R \quad (26)$$

for some upper-triangular R . It then follows

$$[T]_\beta = R[T]_\gamma R^{-1} \quad (27)$$

and every matrix on the right hand side is upper-triangular, hence so is $[T]_\beta$.

Therefore it remains to show we can always choose such γ . This is proven in the homework, but I will include it. This is from Kevin Purbhoo's solution.

We proceed by Strong induction on $\dim V$. If $\dim V = 1$ the result is obvious. Assume $\dim V > 2$ and the result holds for $\dim V < n$, then for $\dim V = n$, consider a proper T -invariant subspace W of V . By hypothesis, there exists $\eta = \{w_1, \dots, w_l\}$ and $\xi = \{v_1 + W, \dots, v_m + W\}$ bases for W and V/W such that $[T_W]_\eta$ and $[\bar{T}_{V/W}]_\xi$ are upper-triangular (for some l, m)¹⁰. By proposition 2.5, $\chi = \eta \cup \xi$ is a basis for V . By Theorem 2.7, $[T]_\chi$ is block upper-triangular. But since all its diagonal blocks are upper-triangular, so is $[T]_\chi$. Hence we can choose $\gamma = \chi$, and this completes the proof. □

The most useful application of the Gram-Schmidt process is the QR-Decomposition. It is very important for computational purposes, especially for those of eigenvalues. It is so important practically, that we, theoretical students, do not necessarily give a single **** at the stage.

4.3 The Hermitian Adjoint

Recall the transpose operator defined in Theorem 2.10, there is an inner product version of it with much simpler representations. Notice that the Hermitian Adjoint for a matrix is already defined in Proposition 4.6, and we are going to provide an operator version of it.

Definition 4.20 (Hermitian Adjoint). *Let V, W be inner product spaces, and $T \in \mathcal{L}(V, W)$, then the **Hermitian Adjoint** of T , $T^* \in \mathcal{L}(W, V)$, is the linear map with the property that for all $v \in V$ and $w \in W$,*

$$\langle Tv, w \rangle_W = \langle v, T^*w \rangle_V \quad (\odot)$$

¹⁰The greek letters have nothing to do specifically, forget them.

Proposition 4.21 (Highlander's Theorem). *Following the notations from Definition 4.20,*

1. T^* is unique if it exists.
2. For $U \in \mathcal{L}(X, V)$, $(TU)^* = U^*T^*$.
3. For $k \in \mathbb{C}$, $U \in \mathcal{L}(V, W)$, $(T + kU)^* = T^* + \bar{k}U^*$.
4. $(T^*)^* = T$

Proof. 1. Assume T' is another adjoint of T , then for all $v \in V$ and $w \in W$,

$$\langle Tv, w \rangle_W = \langle v, T^*w \rangle_V = \langle v, T'w \rangle_V \iff \langle v, (T^* - T')w \rangle_V = 0 \iff T^* = T' \quad (28)$$

Hence T^* is unique.

2. For $x \in X$, $v \in V$ and $w \in W$,

$$\langle TUx, w \rangle_W = \langle Ux, T^*w \rangle_V = \langle x, U^*T^*w \rangle_X \quad (29)$$

Hence $(TU)^* = U^*T^*$.

3. For $v \in V$, $w \in W$,

$$\begin{aligned} \langle (T + kU)v, w \rangle_W &= \langle Tv, w \rangle_W + \langle kUv, w \rangle_W = \langle v, T^*w \rangle_V + \langle v, (kU)^*w \rangle_V \\ &= \langle v, T^*w \rangle_V + \langle v, \bar{k}U^*w \rangle_W = \langle v, (T^* + \bar{k}U^*)w \rangle_V \end{aligned} \quad (30)$$

Hence $(T + kU)^* = T^* + \bar{k}U^*$.

4. For $v \in V$, $w \in W$,

$$\langle T^*w, v \rangle_V = \overline{\langle v, T^*w \rangle_V} = \overline{\langle Tv, w \rangle_W} = \langle w, Tv \rangle_W \quad (31)$$

Hence $(T^*)^* = T$.

□

Now we reveal the connection of this Hermitian adjoint to the one with matrix defined earlier.

Theorem 4.22. *Let V, W be finite-dimensional inner product space, and β, γ orthonormal bases for V, W respectively. Let $T \in \mathcal{L}(V, W)$, then T^* exists, and*

$$[T^*]_{\gamma}^{\beta} = \left([T]_{\beta}^{\gamma}\right)^* \quad (\star)$$

Proof. In order to prove everything, we can start with (\star) as the definition of T^* and show (\odot) holds. Let $\beta = v_1, \dots, v_n$ and $\gamma = w_1, \dots, w_m$. Let $x = \sum_{i=1}^n a_i v_i$ and $y = \sum_{i=1}^m b_i w_i$. Then

$$\langle Tx, y \rangle = \sum_{i=1}^n \sum_{j=1}^m a_i \bar{b}_j \langle Tv_i, w_j \rangle \quad (32)$$

We claim that $\langle Tv_i, w_j \rangle = \left([T]_{\beta}^{\gamma}\right)_{ji}$. Write $Tv_i = \sum_{i=1}^m c_i w_i$, then

$$\langle Tv_i, w_j \rangle = \left\langle \sum_{i=1}^m c_i w_i, w_j \right\rangle = c_j \langle w_j, w_j \rangle = c_j \quad (33)$$

Therefore

$$\langle Tx, y \rangle = \sum_{i=1}^n \sum_{j=1}^m a_i \bar{b}_j \left([T]_{\beta}^{\gamma} \right)_{ji} \quad (34)$$

On the other hand,

$$\langle x, T^*y \rangle = \left\langle \sum_{i=1}^n a_i v_i, \sum_{j=1}^m b_j T^*w_j \right\rangle = \sum_{i=1}^n \sum_{j=1}^m a_i \bar{b}_j \langle v_i, T^*w_j \rangle = \sum_{i=1}^n \sum_{j=1}^m a_i \bar{b}_j \overline{\langle T^*w_j, v_i \rangle} \quad (35)$$

Similarly, write $T^*w_j = \sum_{i=1}^n d_i v_i$, and

$$\langle T^*v_i, v_j \rangle = \left\langle \sum_{i=1}^n d_i v_i, v_j \right\rangle = d_j \quad (36)$$

Thus $\langle v_i, T^*w_j \rangle = ([T^*]_{\gamma}^{\beta})_{ij}$. Hence it follows that

$$\langle Tx, y \rangle = \sum_{i=1}^n \sum_{j=1}^m a_i \bar{b}_j \left([T]_{\beta}^{\gamma} \right)_{ji} = \sum_{i=1}^n \sum_{j=1}^m a_i \bar{b}_j \left([T^*]_{\gamma}^{\beta} \right)_{ij} = \langle x, T^*y \rangle \quad (37)$$

as desired, and the proof is complete. \square

Remark. Notice that in the above proof, the inner products in V and W are used interchangeably due to my laziness, but you should be able to identify which one is which in the context.

Here we demonstrate a key point of the adjoint. If we use orthonormal basis, then the problems of operator sthat have to do with inner products are reflected by their matrix representations. Theoretically, therefore, one might want to use an orthonormal basis whenever dealing with an inner product space.

Definition 4.23 (Self-adjoint Operator). *Let V be an inner product space over \mathbb{F} , $T \in \mathcal{L}(V)$. T is called a **self-adjoint operator** if $T = T^*$. If $\mathbb{F} = \mathbb{R}$, T is called a **symmetric operator**, and if $\mathbb{F} = \mathbb{C}$, T is called a **Hermitian operator**.*

We then have the following corollary to Theorem 4.22.

Corollary 4.24. *Let V be a finite-dimensional inner product space, β be an orthonormal basis for V , and $T \in \mathcal{L}(V)$. Then T is self-adjoint if and only if $A = A^*$, where $A = [T]_{\beta}$.*

Proof. Obvious. \square

I apologize for the rest of this section because my handwritten notes are completely indecipherable.

Example. If $A \in M_{n \times n}(\mathbb{F})$ is self-adjoint, then $L_A : \mathbb{F}^n \rightarrow \mathbb{F}^n$ given by $L_A(x) = Ax$ is a self-adjoint linear operator.

Example. If V is a finite-dimensional inner product space, $W \subseteq V$. Then P_W is self-adjoint.

To see this, recall from Theorem 4.18, $x = P_W x + P_{W^\perp} x$, hence

$$\langle P_W x, y \rangle = \langle P_W x, P_W y + P_{W^\perp} y \rangle = \langle P_W x, P_W y \rangle = \langle x, P_W y \rangle \quad (38)$$

Therefore $(P_W)^* = P_W$.

Example. If V, W are finite-dimensional inner product spaces, $T \in \mathcal{L}(V, W)$. Then $T^*T \in \mathcal{L}(V)$ is self-adjoint, since

$$\langle T^*Tx, y \rangle = \langle Tx, T^{**}y \rangle = \langle Tx, Ty \rangle = \langle x, T^*Ty \rangle \quad (39)$$

Recall a familiar and important result in linear algebra that if T and U are linear maps properly defined, then $\text{rank}(UT) \leq \min\{\text{rank}(U), \text{rank}(T)\}$. We have the following result for adjoints.

Theorem 4.25. Let V, W be finite-dimensional inner product space, $L \in \mathcal{L}(V, W)$. Then

$$\text{rank}(T) = \text{rank}(T^*T) = \text{rank}(TT^*) = \text{rank}(T^*)$$

Proof. Clearly $\text{rank}(T^*) = \text{rank}(T)$. Clearly $\dim \ker T^*T \geq \dim \ker T$. Suppose now $x \in \ker T$, then

$$T^*Tx = 0 \implies \langle T^*Tx, x \rangle = 0 \implies \langle Tx, Tx \rangle = 0 \quad (40)$$

By definition, $Tx = 0$ and hence $\ker T = \ker T^*T$. The rest follows. \square

The following example is inserted to demonstrate that the projection is not well-defined sometimes

Example. Consider $V = \mathbb{R}[t]$, and the inner product

$$\langle f, g \rangle = \sum_{i=0}^{\infty} a_i b_i \quad (41)$$

where $f(t) = \sum_{i=0}^k a_i t^i$ and $g(t) = \sum_{i=0}^l b_i t^i$. It is easy to see that $\beta = \{1, t, t^2, \dots\}$ is an orthonormal basis for V . Consider the subspace

$$W = \{g(t) \in V \mid g(1) = 0\} \quad (42)$$

We claim that P_W is not defined.

For any $x \in V$, for P_W to exist, we need $x - P_W x \in W^\perp$ and $P_W x \in W$. We claim that $f(t) \in W^\perp \implies f(t) \equiv 0$.

Suppose $f(t) \in V$ and $f \neq 0$, write $f(t) = \sum_{i=0}^n a_i t^i$. Consider $g(t) = f(t) - f(1)t^{n+1}$. Clearly $g(1) = 0 \implies g(t) \in W$, and

$$\langle f(t), g(t) \rangle = \langle f(t), f(t) \rangle - f(1)\langle f(t), t^{n+1} \rangle = \langle f(t), f(t) \rangle > 0 \quad (43)$$

Thus $f(t) \notin W^\perp$, and it follows $W^\perp = \{0\}$.

On the other hand, $x - P_W x = 0 \implies P_W x = x \implies x \in W$ for all $x \in V$. Then $W = V$, contradiction. Hence P_W does not exist.

So what is, after all, so useful about the Hermitian adjoint of operators? We will see in the next few demonstrations.

Proposition 4.26. There will be a midterm on Thursday, Nov. 12, 2015.

Proof. Assume the contrary that there is not a midterm on the given day. By assumption, you do not have to go to the assigned room on that day. Empirically, after a period of time it is certain that you will find on your transcript a lower degree than expected, contradiction. Notice that the expected grade of midterm will be non-zero since Kevin Purbhoo curves the exam, historically. \square

Alright, what is actually useful will be the following, the least square approximation.

Consider $A \in M_{m \times n}(\mathbb{F})$, and the equation $Ax = b$ for some $b \in \mathbb{F}^m$. This is not generally solvable, but it is always possible to find an x that minimizes¹¹

$$\|Ax - b\| \quad (44)$$

Now if you are a legitimate MATH 247 student, you will take the derivative of this function, find the critical points, compute the Hessian, and show that it is positive definite. However, there is an easy way of doing this.

¹¹ "This function is strictly convex" - D. Siegel

Theorem 4.27. (44) is minimized if and only if x is a solution to the equation

$$A^*Ax = A^*b$$

Moreover, if $\text{rank}(A) = n$, then by Theorem 4.25, $\text{rank}(A^*A) = n$, hence it is invertible, and therefore x can be uniquely determined by $(A^*A)^{-1}A^*b$.

Proof. Recall Theorem 4.13, to minimize (44), we want Ax to be $\text{Proj}_{\text{Col}(A)}(b)$, we will show that the above is true when $A^*Ax = A^*b$. Clearly $Ax \in \text{Col}(A)$. Also

$$A^*b = A^*Ax \implies b - Ax \in \text{Null}(A^*) \implies b - Ax \in \text{Col}(A)^\perp \quad (45)$$

Hence $Ax = \text{Proj}_{\text{Col}(A)}(b)$.

Conversely, if $Ax = \text{Proj}_{\text{Col}(A)}(b)$, then $b - Ax \in \text{Null}(A^*)$, and $A^*(b - Ax) = 0 \implies A^*Ax = A^*b$. The rest follows. \square

Corollary 4.28. If $\text{rank}(A) = n$, then

$$A(A^*A)^{-1}A^* = \text{Proj}_{\text{Col}(A)}$$

Proof. Follows directly from Theorem 4.28. \square

Remark. The matrix $(A^*A)^{-1}A^*$ is called the pseudoinverse of A . This definition only makes sense when $\text{rank}(A) = n$.

Now it is time to explain why the least square is good for statistics. Consider data points $(a_1, b_1), \dots, (a_m, b_m)$, and we want to find a line that is a good approximation for the data. That will be a line that minimizes the sum of distances from the data points to the line. Let $y = cx + d$, and we wish to minimize

$$\sum_{i=1}^m (b_i - (cx_i + d))^2 \quad (46)$$

If we take

$$A = \begin{pmatrix} a_1 & b_1 \\ \vdots & \vdots \\ a_m & b_m \end{pmatrix}, \quad x = \begin{pmatrix} c \\ d \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

The problem is equivalent to minimize

$$\|Ax - b\|^2 \quad (47)$$

which can be done with the method introduced above.

Insert remote-control car example here, why would I even care?

4.4 Normal Operators

“This is probably one of the worst named thing.”

—Kevin Purbhoo, 2015

Definition 4.29 (Normal Operator). Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$. We say T is **normal** if $TT^* = T^*T$. Similarly, a matrix $A \in M_{n \times n}(\mathbb{F})$ is normal if $AA^* = A^*A$.

Example. Diagonal matrices are normal. This is obvious.

Example. Self-adjoint matrices are normal.

Example. If $A = A^*$, then A is normal. They are called skew-symmetric matrices over \mathbb{R} or skew-Hermitian matrices over \mathbb{C} .

Example. If $A^* = A^{-1}$, then A is normal. They are called orthonormal matrices over \mathbb{R} or unitary matrices over \mathbb{C} .

Example. If $A^* = -A^{-1}$, then A is normal. However such matrix does not exist.

Below are some basic properties.

Theorem 4.30. *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$. Then*

1. $\|Tx\| = \|T^*x\|$ for $x \in V$
2. $T - uI$ is normal for $u \in \mathbb{F}$.
3. if x is an eigenvector of T with eigenvalue λ , then $T^*x = \bar{\lambda}x$. Moreover, if λ_i and λ_j are different eigenvalues for T , then $E_{\lambda_i} \perp E_{\lambda_j}$ for $i \neq j$.

Proof. We prove 1 first,

$$\|Tx\| = \langle Tx, Tx \rangle = \langle x, T^*Tx \rangle = \langle x, TT^*x \rangle = \langle T^*x, T^*x \rangle = \|T^*x\| \quad (48)$$

as desired. To see 2, we have

$$\begin{aligned} (T - uI)(T - uI)^* &= (T - uI)(T^* - \bar{u}I) = TT^* - uT^* - \bar{u}T + u\bar{u} \\ &= T^*T - uT^* - \bar{u}T + u\bar{u} = (T^* - \bar{u}I)(T - uI) = (T - uI)^*(T - uI) \end{aligned} \quad (49)$$

For 3, let $U = T - \lambda I$, then $U^* = T^* - \bar{\lambda}I$. Hence

$$Tx = \lambda x \implies Ux = 0 \implies \|Ux\| = 0 \implies \|U^*x\| = 0 \implies T^*x = \bar{\lambda}x \quad (50)$$

For 4, let $x_i \in E_{\lambda_i}$ and $x_j \in E_{\lambda_j}$. Then

$$\lambda_i \langle x_i, x_j \rangle = \langle \lambda_i x_i, x_j \rangle = \langle Tx_i, x_j \rangle = \langle x_i, T^*x_j \rangle = \langle x_i, \bar{\lambda}_j x_j \rangle = \lambda_j \langle x_i, x_j \rangle \quad (51)$$

Since the eigenvalues are distinct, $\langle x_i, x_j \rangle = 0$ as desired. \square

There are some nice results on diagonalizability of normal operators as well. We start this by a lemma on normal matrices.

Lemma 4.31. *Let $X \in M_{n \times n}(\mathbb{F})$. If $X = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, where $A \in M_{k \times k}(\mathbb{F})$ and $C \in M_{(n-k) \times (n-k)}(\mathbb{F})$ then X is normal if and only if A and C are normal and $B = 0$.*

Proof. If A and C are normal and $B = 0$, then X is diagonal with two normal operators on its diagonal. Therefore X is clearly normal.

On the other hand, we shall directly compute X^*X and XX^* . We have

$$X^*X = \begin{pmatrix} A^*A & A^*B \\ B^*A & B^*B + C^*C \end{pmatrix} \text{ and } XX^* = \begin{pmatrix} AA^* + BB^* & BC^* \\ CB^* & CC^* \end{pmatrix} \quad (52)$$

Since X is normal,

$$XX^* = X^*X \iff A^*A = AA^* + BB^* \iff \text{tr}(A^*A) = \text{tr}(AA^*) + \text{tr}(BB^*) \quad (53)$$

By Proposition 4.6, $\text{tr}(AA^*)$ is a well-defined inner product, thus it follows that $\text{tr}(A^*A) = \text{tr}(AA^*) \implies \text{tr}(BB^*) = 0 \implies \langle B, B \rangle = 0 \implies B = 0$. Hence $AA^* = A^*A$, and A is normal. Similarly, C is normal and the proof is complete. \square

Theorem 4.32. *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$ a normal operator. If $f_T(t)$ splits, then there exists an orthonormal basis β of eigenvectors of T .*

Proof. By Schur's theorem, there exists an orthonormal basis β such that $X = [T]_\beta$ is upper-triangular. Since T is normal, it follows that X is also normal since

$$XX^* = [T]_\beta [T^*]_\beta = [TT^*]_\beta = [T^*T]_\beta = [T^*]_\beta [T]_\beta = X^*X \quad (54)$$

Hence X is block upper-triangular in many ways. By Lemma 4.32, all k by $(n-k)$ upper blocks is identically 0 for all proper k . If we range k through all possible values, we see that X is indeed diagonal.

On the other hand, if β is an orthonormal basis and $[T]_\beta$ is diagonal, then it automatically follows that β consists of eigenvectors and since each diagonal block is normal, T is normal since diagonal matrices are normal if β is orthonormal.¹² \square

Again, we have the following theorem on invariant subspaces.

Theorem 4.33. *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$ a normal operator. If W is a T -invariant subspace of V , then W^\perp is T -invariant and $T_W^* = (T^*)_W$.*

Proof. Essentially, since W is T -invariant, by Proposition 2.7, we can put T in block upper-triangular form. Since $W \oplus W^\perp = V$, it also means that T can be put in block diagonal form, by Lemma 4.32. Say $[T]_\beta = \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}$ for some orthonormal basis β , then since A is also normal, it follows that $T_W^* = (T^*)_W$. \square

Remark. Notice that it also follows in a similar fashion that $T_{W^\perp}^* = (T^*)_{W^\perp}$.

In general, if T is not normal, it is possible to have a T -invariant subspace W such that there does not exist another invariant subspace W' with $T = W \oplus W'$.

In fact, if T is normal, we can let β and γ be orthonormal bases for W and W^\perp respectively. Then $[T]_{\beta \cup \gamma}$ is block upper-triangular. It is also normal since T is normal. By Lemma 4.32, $[T]_\beta$ is indeed block diagonal, and W^\perp is also T -invariant. The next theorem is nothing but a revision and extension of the previous theorems. It is more notable that this theorem has a name while others do not.

Theorem 4.34 (Spectral Theorem). *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$ a normal operator. Suppose $f_T(t)$ splits. Let $\lambda_1, \dots, \lambda_k$ be distinct eigenvalues of T , then*

1. $T = \sum_{i=1}^k \lambda_i \text{Proj}_{E_{\lambda_i}}$.
2. $I = \sum_{i=1}^k \text{Proj}_{E_{\lambda_i}}$.
3. $\text{Proj}_{E_{\lambda_i}} \text{Proj}_{E_{\lambda_j}} = 0$ for $i \neq j$.

Proof. By Theorem 4.32, T is diagonalizable, and

$$V = \bigoplus_{i=1}^k E_{\lambda_i} \quad (55)$$

Let $x \in V$, then $x = \sum_{i=1}^k a_i x_i$, for $x_i \in E_{\lambda_i}$. By Theorem 4.31, $E_{\lambda_i} \perp E_{\lambda_j}$ for $i \neq j$. So for each i , by Theorem 4.13,

$$x_i = \text{Proj}_{E_{\lambda_i}}(x) \implies \sum_{j=1}^k x_j - x_i \in E_{\lambda_i}^\perp \quad (56)$$

¹²I have no idea why this paragraph is here since it seems unrelated to the original theorem, but its on my notes.

Therefore

$$x = \sum_{i=1}^k \text{Proj}_{E_{\lambda_i}}(x) \implies I = \sum_{i=1}^k \text{Proj}_{E_{\lambda_i}} \quad (57)$$

and

$$Tx = \sum_{i=1}^k T \text{Proj}_{E_{\lambda_i}}(x) = \sum_{i=1}^k \lambda_i \text{Proj}_{E_{\lambda_i}}(x) \implies T = \sum_{i=1}^k \lambda_i \text{Proj}_{E_{\lambda_i}} \quad (58)$$

The above completes 1) and 2). To prove 3), simply notice that $E_{\lambda_i} \perp E_{\lambda_j}$ for $i \neq j$, and by Proposition 4.17, $\text{Proj}_{E_{\lambda_i}} \text{Proj}_{E_{\lambda_j}} = 0$ for $i \neq j$, as desired. \square

Remark. The above theorem can be reformulated in terms of projections as well, but I don't know how to do it so I might as well omit it.

What happens to the diagonalizability of self-adjoint operators? Well as it turns out, something pretty deep can happen¹³.

Theorem 4.35. *Let V be a finite-dimensional inner product space over \mathbb{F} , $T \in \mathcal{L}(V)$ a self-adjoint operator. There exists an orthonormal basis β of eigenvectors such that $[T]_{\beta}$ is diagonal. Moreover, all eigenvalues are real.*

If $\mathbb{F} = \mathbb{R}$ and T is diagonalizable by an orthonormal basis, then $T = T^$.*

Proof. The first case is when $\mathbb{F} = \mathbb{C}$. By the fundamental theorem of algebra, $f_T(t)$ splits. By Theorem 4.34, T is diagonalizable, say $T = Q^T D Q$ for some diagonal D . $T = T^* \implies D = D^*$, since D is diagonal with entries eigenvalues of T , we see that all eigenvalues are real.

For the real case, we can let γ be any orthonormal basis of V . Since T is self-adjoint, it follows that $[T]_{\gamma} = [T]_{\gamma}^*$. From the complex case, we see that $[T]_{\gamma}$ has real eigenvalues, and therefore $f_T(t)$ splits. Hence T is diagonalizable by an orthonormal basis.

Conversely, if β is orthonormal and $[T]_{\beta}$ is diagonal, $[T]_{\beta}$ is also self-adjoint since entries of $[T]_{\beta}$ are real. It follows that T is self-adjoint as well. \square

4.5 Unitary Matrices

When we are diagonalizing normal matrices, we essentially get 1 by 1 matrices that are normal. Similarly when we are diagonalizing self-adjoint matrices, we get 1 by 1 matrices that are self-adjoint. Note that the above is meaningless when we talk about real numbers, but in complex numbers it is somewhat deep as it shows that all eigenvalues are actually real (not as in, they exist). Same philosophy applies to unitary and skew-symmetric(Hermitian) matrices. The pattern persists for blocks as well.

Now let us actually do stuff for unitary matrices (The definition appears in Definition 4.30).

Theorem 4.36. *Let V be a finite-dimensional inner product space, $T \in \mathcal{L}(V)$ a unitary operator. There exists orthonormal basis β such that $[T]_{\beta}$ is diagonal, and every eigenvalue of T is a complex number λ such that $||\lambda|| = 1$.*

Proof. Since T is unitary, T is also normal, thus by Theorem 4.33, β exists and $[T]_{\beta} = D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$.

Since T is unitary, D is also unitary, and it follows $I = DD^* = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \begin{pmatrix} \overline{\lambda_1} & & \\ & \ddots & \\ & & \overline{\lambda_n} \end{pmatrix}$. Hence

$||\lambda_i|| = 1$ for all i . \square

¹³as they always happen, because they are deep.

In the real case intuitively we would expect orthogonal operators to exhibit similar properties, but the above theorem fail miserably for real numbers as orthogonal operators are not necessarily diagonalizable. For example, consider the rotation matrix (counterclockwise with angle θ):

$$Q = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad (59)$$

There is no eigenvalue for in general for Q with the exception of $\theta = k\pi$ for $k \in \mathbb{Z}$, and therefore Q is certainly not diagonalizable.

So what can we do to orthogonal matrices when they are not diagonalizable? In Chapter 3 we used Canonical forms, they can certainly be put into those forms, but the problem is that the basis might not be orthonormal and that is no ideal. As it turns out, however, these matrices are almost diagonalizable by an orthonormal basis. We have the following Canonical Form for real orthogonal operators (to be proved later).

If T is an orthogonal operator, then there exists orthonormal basis β such that

$$[T]_{\beta} = \begin{pmatrix} Q_1 & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_k \end{pmatrix} \quad (60)$$

where each Q_i is either 1 or -1 or a rotation matrix (orthogonal matrix with determinant 1) for $\theta_i \notin \pi\mathbb{Z}$

$$\begin{pmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{pmatrix} \quad (61)$$

We see that $[T]_{\beta}$ is block diagonal and is almost diagonal since each block is either 1 by 1 or 2 by 2.

Before proving the above theorem, we shall prove some nice results about unitary/orthogonal operators.

Theorem 4.37. *Let V be a finite-dimensional vector space over \mathbb{F} , $T \in \mathcal{L}(V)$. The following are equivalent:*

1. $TT^* = T^*T = I$.
2. $\langle Tx, Ty \rangle = \langle x, y \rangle$ for all $x, y \in V$.
3. If β is an orthonormal basis for V , then so is $T\beta$.
4. There exists an orthonormal basis such that $T\beta$ is orthonormal.
5. $\|Tx\| = \|x\|$ for all $x \in V$.

Proof. 1 \implies 2.

$$\langle Tx, Ty \rangle = \langle x, T^*Ty \rangle = \langle x, y \rangle \quad (62)$$

2 \implies 3. Suppose $\beta = \{\beta_1, \dots, \beta_n\}$, then $T\beta = \{T\beta_1, \dots, T\beta_n\}$ and

$$\langle \beta_i, \beta_j \rangle = \delta_{ij} \implies \langle T\beta_i, T\beta_j \rangle = \delta_{ij} \quad (63)$$

where δ_{ij} is the Kronecker delta.

3 \implies 4. Trivial.

4 \implies 5. Suppose β and $T\beta$ are both orthonormal bases for V . Let $x = \sum_{i=1}^n a_i \beta_i$, then

$$\|Tx\| = \left\| \sqrt{\sum_{i=1}^n a_i^2} \right\| = \|x\| \quad (64)$$

5 \implies 1. Since T^*T is self-adjoint, by Theorem 4.36, there exists $\beta = \{\beta_1, \dots, \beta_n\}$ an orthonormal basis for V consisting of eigenvalues of T^*T . Let $\lambda_1, \dots, \lambda_n$ be the corresponding eigenvalues, then

$$\|\beta_i\|^2 = \|T\beta_i\|^2 = \langle T\beta_i, T\beta_i \rangle = \langle T^*T\beta_i, \beta_i \rangle = \lambda_i \langle \beta_i, \beta_i \rangle = \lambda_i \|\beta_i\|^2 \quad (65)$$

Thus $\lambda_i = 1$ for all i , and it follows that T^*T is the identity. \square

Remark. Notice that if V is not finite-dimensional, then 5 does not imply 1. In fact it does not even imply T is normal.

Theorem 4.38. *Let $Q \in M_{n \times n}(\mathbb{F})$ be unitary if $\mathbb{F} = \mathbb{C}$ or orthogonal if $\mathbb{F} = \mathbb{R}$. The columns of Q form an orthonormal basis for \mathbb{F}^n .*

Proof. Let $\{e_1, \dots, e_n\}$ be the standard orthonormal basis for \mathbb{F}^n . By the previous theorem, $\{Qe_1, \dots, Qe_n\}$ is an orthonormal basis for \mathbb{F}^n as well, but at the same time they are the columns of Q , and the proof is complete. \square

It looks like that is enough for today. Um, uhh, nah let us say a few more things.

Corollary 4.39. *$A \in M_{n \times n}(\mathbb{C})$ is normal if and only if there exists a unitary matrix Q and a diagonal matrix D such that $A = QDQ^*$*

Corollary 4.40. *$A \in M_{n \times n}(\mathbb{R})$ is self-adjoint if and only if there exists an orthogonal matrix Q and a diagonal matrix D such that $A = QDQ^T$.*

Proof. They follow as a consequence of Theorem 4.33, Theorem 4.36 and the previous theorem. The converse is direct computation. \square

As promised, we shall be investigating diagonalizability of normal matrices over the real numbers.

Theorem 4.41 (Canonical Form for Normal Matrices over \mathbb{R}). *Let V be a finite-dimensional vector space over \mathbb{R} , $T \in \mathcal{L}(V)$ a normal operator. There exists basis β such that*

$$[T]_\beta = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{pmatrix}$$

where $A_i = \lambda_i$ for some $\lambda_i \in \mathbb{R}$ or $A_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$ for some $a_i, b_i \in \mathbb{R}$ and $b_i \neq 0$.

Proof. We claim that $m_T(t)$ is square-free first. It is enough to prove for normal matrices A instead.

If A is normal over \mathbb{R} , it is also normal over \mathbb{C} . By Theorem 4.33, A is diagonalizable over \mathbb{C} . By Theorem 3.9, $m_A(t)$ is square-free. The minimal polynomial does not change over \mathbb{R} , and therefore it is square-free over \mathbb{R} as well (It might not split).

Now to prove the original theorem, we first notice that $f_T(t)$ factors into linear or quadratic terms (Essentially, this is saying that all roots of the characteristic polynomial appear either in a real number or a pair of complex numbers that are conjugate of each other). Let γ be any rational canonical basis for T , then $[T]_\gamma$ is block diagonal with each diagonal block R_i a companion matrix with minimal polynomial $q_i(t)^{d_i}$ irreducible over \mathbb{R} . Since $m_T(t)$ is square free, $q_i(t)^{d_i} \mid m_T(t) \implies d_i = 1$. Therefore all blocks are 1 by 1 or 2 by 2 matrices.

Apply Gram-Schmidt to γ . Let β be the output, we claim that this β is the desired basis. We have $[T]_\beta = Q[T]_\gamma Q^{-1}$ for some upper-triangular invertible Q . Therefore $[T]_\beta$ is block upper-triangular. By Lemma 4.32, since T is normal, $[T]_\beta$ is actually block diagonal with each block 1 by 1 or 2 by 2 with irreducible characteristic polynomial $q_i(t)$. If a block is 1 by 1 then it follows that it is an eigenvalue of T . Otherwise a block will be a 2 by 2 matrix that is not diagonalizable, which is of the form

$$A_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix} \quad (66)$$

for some $a_i, b_i \in \mathbb{R}$ and $b_i \neq 0$.

To see this, let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a normal matrix, then

$$AA^T = A^T A \iff b = c \vee (b = -c \wedge a = d) \quad (67)$$

If $b = c$, by Theorem 4.36, A is diagonalizable. Hence $b = -c$ and $a = d$, which results in the above form as a consequence, and the proof is complete. \square

Remark. The canonical form for orthogonal matrix is a special case of the above theorem. Since the determinant of an orthogonal matrix is ± 1 , the eigenvalues are either 1 or -1 , it follows that for any A_i , $|\det(A_i)| = 1 \implies a_i^2 + b_i^2 = 1$ (it simply cannot be -1 !). So we can write it using trigonometric functions.

We also have the following unproven random theorem.

Theorem 4.42. *Let V be a finite-dimensional inner product space over \mathbb{F} , $T \in \mathcal{L}(V)$. There exists a basis β such that $[T]_\beta$ is block upper-triangular and the characteristic polynomial of each diagonal block is an irreducible factor $f_T(t)$.*

Proof. I do not know how to prove this. I think this is not important anyways. \square

What happens if we want to somehow make any linear operator somewhat diagonal? It turns out for any vector space V and W over \mathbb{F} and $T \in \mathcal{L}(V, W)$, there exist bases β and γ for V and W respectively such that (note the matrix below is a rough sketch of what is actually happening)

$$[T]_\beta^\gamma = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & \vdots \\ & & 0 & 0 \end{pmatrix} \quad (68)$$

That is, on the main diagonal there are k 1's, where $k = \text{rank } T$, and 0 everywhere else.

To achieve this, we can pick $\beta' = \{x_1, \dots, x_l\}$ a basis for $\ker T$ and extend it to $\beta = \{y_1, \dots, y_k, x_1, \dots, x_l\}$. Compute $\gamma' = \{Ty_1, \dots, Ty_k\}$ and extend it to a basis γ for W . Convince yourself that this choice of bases works.

The real question is what if we want to use orthonormal bases instead if $\mathbb{F} = \mathbb{C}$ or \mathbb{R} ? It turns out that we can not make the diagonal into 1's anymore. Instead we get the so-called singular values $\sigma_1, \dots, \sigma_k$ on the diagonal and 0 everywhere else. This is the singular value decomposition (SVD). The SVD, together with the QR decomposition, are two of the most important tools in computational linear algebra. Meanwhile, they are also two of the things we do not care about.

4.6 Bilinear Forms over Other Fields

In this section, \mathbb{F} will be any field unless otherwise specified.

We assume that $\text{char}(\mathbb{F}) \neq 2$. Let V be a vector space over \mathbb{F} , recall that a bilinear form $H : V \times V \rightarrow \mathbb{F}$ is symmetric if $H(x, y) = H(y, x)$ for all $x, y \in V$, is anti-symmetric if $H(x, y) = -H(y, x)$ for all $x, y \in V$, and is non-degenerate if $H(x, y) = H(x, z) \implies y = z$ for all $x, y, z \in V$ and $x \neq 0$.

Definition 4.43 (Quadratic Form). *Let V be a vector space over \mathbb{F} , $H : V \times V \rightarrow \mathbb{F}$ a bilinear form. The associated **quadratic form** is $K(x) = H(x, x)$.*

There are many useful identities of $K(x)$. K is called a quadratic form since $K(\alpha x) = \alpha^2 K(x)$ for all $\alpha \in \mathbb{F}$. Moreover given any quadratic form $K(x)$, the corresponding bilinear form is given by

$$H(x, y) = \frac{1}{2}(K(x+y) - K(x) - K(y)) \quad (69)$$

We also have the matrix representation of a bilinear form.

Theorem 4.44. Let V be a finite-dimensional vector space over \mathbb{F} , $H : V \times V \rightarrow \mathbb{F}$ a bilinear form. There is a basis $\beta = \{v_1, \dots, v_n\}$ for V such that $[H]_\beta = [H]_{\beta, \beta}$ is unique and satisfies

$$H(x, y) = ([x]^\beta)^T [H]_\beta [y]^\beta$$

and $([H]_\beta)_{ij} = H(v_i, v_j)$.

Proof. Assume first such representation exists, then we must have

$$H(v_i, v_j) = ([v_i]^\beta)^T [H]_\beta [v_j]^\beta = e_i^T [H]_\beta e_j = ([H]_\beta)_{ij} \quad (70)$$

We then define $[H]_\beta$ to be the matrix with $([H]_\beta)_{ij} = H(v_i, v_j)$. By bilinearity, we can check this definition is legitimate for all $x, y \in V$. \square

Remark. The letter H is determine by K. Purbhoo. This matrix representation is much easier to calculate that that of a linear operator. They also have different change of basis formula, as we will see later.

Example. Let H be the standard dot product in \mathbb{R}^2 and $\beta = \{(1, 2)^T, (3, 4)^T\}$, then

$$[H]_\beta = \begin{pmatrix} 5 & 11 \\ 11 & 25 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \quad (71)$$

The above example suggests following change of basis formula.

Theorem 4.45. Let V be a finite-dimensional vector space over \mathbb{F} , $H : V \times V \rightarrow \mathbb{F}$ a bilinear form. If β and γ are both bases for V , then

$$[H]_\beta = Q^T [H]_\gamma Q$$

where $\Psi_\beta = \Psi_\gamma Q$.

Proof. By Theorem 4.46,

$$H(x, y) = ([x]^\beta)^T [H]_\beta [y]^\beta \quad (72)$$

$$H(x, y) = ([x]^\gamma)^T [H]_\gamma [y]^\gamma \quad (73)$$

Therefore

$$([H]_\beta)_{ij} = H(v_i, v_j) = H\left(\sum_{k=1}^n Q_{ki} w_k, \sum_{k=1}^n Q_{kj} w_k\right) = \sum_{k=1}^n \sum_{l=1}^n Q_{ik} Q_{lj} ([H]_\gamma)_{kl} = (Q^T [H]_\gamma Q)_{ij} \quad (74)$$

as desired, where $\beta = \{v_1, \dots, v_n\}$ and $\gamma = \{w_1, \dots, w_n\}$. \square

The change of basis formula uses transpose instead of inverse. Nevertheless Q is invertible.

Definition 4.46 (Congruent Matrices). Two matrices $A, B \in M_{n \times n}(\mathbb{F})$ are congruent over \mathbb{F} if there exists an invertible matrix Q such that $A = Q^T B Q$.

Remark. Similarity of two matrices does not depend on the field, but congruence does depend on the field. In the case that $Q^T Q = I$, similarity and congruence coincide.

We then deal with diagonalizability of symmetric forms.

Theorem 4.47 (Diagonalization Theorem). Let V be a finite-dimensional inner product space over \mathbb{F} , $H : V \times V \rightarrow \mathbb{F}$ a symmetric form. There exists β basis for V such that $[H]_\beta$ is diagonal.

Proof. We proceed by induction on $\dim V$. It is trivial when $\dim V = 0$.

Assume the result holds true for $\dim V = n$. Let $K(x) = H(x, x)$. If $K(x) = 0$ then $H(x) = 0$ and we are done since $[H]_\beta$ is simply the zero matrix. Assume henceforth $K(x) \neq 0$, choose $v \in V$ such that $K(v) = 0$. Consider the set of vectors x in V such that $H(x, v) = 0$, i.e

$$W = \{x \in V \mid H(x, v) = 0\} \quad (75)$$

Clearly $H(\cdot, v) : V \rightarrow \mathbb{F}$ is linear, and $\dim W = \dim V - \text{rank } H(\cdot, v)$. $\text{rank } H(\cdot, v)$ must be 1 since $v \neq \ker H(\cdot, v)$. So $\dim W = \dim V - 1$.

Let $J : W \times W \rightarrow \mathbb{F}$ be the bilinear form given by

$$J(w_1, w_2) = H(w_1, w_2) \quad \forall w_1, w_2 \in W \quad (76)$$

By hypothesis there exists a basis $\gamma = \{w_1, \dots, w_n\}$ such that $[J]_\gamma$ is diagonal. We claim that $\beta = \{v, w_1, \dots, w_n\}$ is the desired basis. We show first that β is indeed a basis for V . It is enough to show that β is linearly independent since the dimension matches. Suppose, for a contradiction that there exists a non-trivial linear combination

$$av + \sum_{i=1}^n b_i w_i = 0 \quad (77)$$

We can apply $H(\cdot, v)$ to both sides. Since $w_i \in \ker H(\cdot, v)$, it follows that $aH(v, v) = 0 \implies a = 0$, absurd. Thus β is a basis for V . Also it is not hard to see that $[H]_\beta$ is diagonal with $([H]_\beta)_{11} = H(v, v)$ followed by $[J]_\gamma$. By induction, the result holds true for all V , and we are done. \square

Remark. If $H(\cdot, \cdot)$ is an inner product and $\mathbb{F} = \mathbb{R}$, $[H]_\beta$ is diagonal if and only if β is an orthogonal basis, and $[H]_\beta$ is the identity if and only if β is an orthonormal basis.

In particular, if we are working in an algebraically closed field, or in particular, \mathbb{C} , we can make the diagonalization even better by putting the diagonal into 0's and 1's.

Theorem 4.48. *Let V be a finite-dimensional inner product space over \mathbb{C} , $H : V \times V \rightarrow \mathbb{C}$ a symmetric form. There exists β basis for V such that*

$$[H]_\beta = \begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}$$

for some $k \in \mathbb{Z}$. Moreover, k is unique and we denote $k = \text{rank } H$.

Proof. By Theorem 4.48, we can choose a basis $\gamma = \{w_1, \dots, w_n\}$ such that $[H]_\gamma$ is diagonal. Arrange, if necessary, γ such that $H(w_i, w_i) \neq 0$ for all $i = 1, \dots, k$. Consider the basis $\beta = \{v_1, \dots, v_n\}$ given by

$$v_i = \begin{cases} \frac{w_i}{\sqrt{H(w_i, w_i)}} & H(w_i, w_i) \neq 0 \\ w_i & \text{otherwise} \end{cases} \quad (78)$$

It is clear that $[H]_\beta$ is diagonal, and $H(v_i, v_i) = H\left(\frac{w_i}{\sqrt{H(w_i, w_i)}}, \frac{w_i}{\sqrt{H(w_i, w_i)}}\right) = 1$, hence $[H]_\beta$ will be in the desired form. Moreover k is unique since $k = \dim V - \dim \ker H(\cdot, \cdot)$. \square

The result is more exciting if we are dealing with reals, because not all vectors are normalizable in the real numbers if H is not an inner product.

Theorem 4.49 (Sylvester's Law of Inertia). *Let V be a finite-dimensional inner product space over \mathbb{R} . Let $H : V \times V \rightarrow \mathbb{R}$ be a symmetric form. There exists integers p and q and a basis β for V such that*

$$[H]_\beta = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Moreover, p and q are unique.

Proof. To prove the existence we use the same technique used in last theorem. Let $\gamma = \{w_1, \dots, w_n\}$ be a basis for V such that $[H]_\gamma$ is diagonal. By rearranging the basis, if necessary, we may assume that $H(v_1, v_i) > 0$

for $i = 1, \dots, p$ and $H(v_i, v_i) < 0$ for $i = p+1, \dots, p+q$ and $H(v_i, v_i) = 0$ for the rest of the indices. Consider $\beta = \{v_1, \dots, v_n\}$ basis for V given by

$$v_i = \begin{cases} \frac{w_i}{\sqrt{|H(w_i, w_i)|}} & i = 1, \dots, p+q \\ w_i & \text{otherwise} \end{cases} \quad (79)$$

It is clear that $[H]_\beta$ is diagonal. For $i = 1, \dots, p$, $H(v_i, v_i) = H\left(\frac{w_i}{\sqrt{|H(w_i, w_i)|}}, \frac{w_i}{\sqrt{|H(w_i, w_i)|}}\right) = 1$. For $i = p+1, \dots, p+q$, $H(v_i, v_i) = H\left(\frac{w_i}{\sqrt{-H(w_i, w_i)}}, \frac{w_i}{\sqrt{-H(w_i, w_i)}}\right) = -1$. The rest is 0, so $[H]_\beta$ is in the desired form.

To prove uniqueness there are 2 cases. If H is non-degenerate, then $H(x, y) = H(x, z) \forall x \implies y = z$. It follows that there is no vector x other than 0 such that $H(x, x) = 0$. Thus $p+q = n$ and $[H]_\beta$ is invertible.

Suppose that there exists $\beta' = \{v'_1, \dots, v'_n\}$ basis for V and $[H]_{\beta'} = \begin{pmatrix} I_{p'} & 0 \\ 0 & -I_{q'} \end{pmatrix}$. We wish to show that $p = p'$ and $q = q'$. Suppose for a contradiction that $p' > p$, then $q' < q$. There exists $x \in \text{Span}\{v'_1, \dots, v'_{p'}\} \cap \text{Span}\{v_{p+1}, \dots, v_n\}$ since $p' + q > n$.

Since $x \in \text{Span}\{v'_1, \dots, v'_{p'}\}$,

$$\begin{aligned} H(x, x) &= ([x]^{\beta'})^T [H]_{\beta'} [x]^{\beta'} = (a_1, \dots, a_{p'}, 0, \dots, 0) \begin{pmatrix} I_{p'} & 0 \\ 0 & -I_{q'} \end{pmatrix} (a_1, \dots, a_{p'}, 0, \dots, 0)^T \\ &= \sum_{i=1}^{p'} a_i^2 > 0 \end{aligned} \quad (80)$$

Again, since $x \in \text{Span}\{v_{p+1}, \dots, v_n\}$,

$$\begin{aligned} H(x, x) &= ([x]^\beta)^T [H]_\beta [x]^\beta = (0, \dots, 0, b_{p+1}, \dots, b_n) \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} (0, \dots, 0, b_{p+1}, \dots, b_n)^T \\ &= \sum_{i=p+1}^n -b_i^2 < 0 \end{aligned} \quad (81)$$

Contradiction.

If H is degenerate, we consider the following subspace

$$W = \{x \in V \mid H(x, y) = 0 \forall y \in V\}$$

and define the symmetric form $\bar{H} : V/W \times V/W \rightarrow \mathbb{R}$ given by $\bar{H}(x+W, y+W) = H(x, y)$ for all $x, y \in V$.

It is clear that \bar{H} is symmetric. We claim that \bar{H} is also non-degenerate. In fact, if $x+W = x'+W$ and $y+W = y'+W$, we have

$$H(x', y') = H(x, y) + H(x' - x, y) + H(x', y' - y) = H(x, y) \quad (82)$$

since $x - x' \in W$ and $y - y' \in W$. Hence if $\bar{H}(x+W, y+W) = 0$ for all y , then $x \in W$. It follows \bar{H} is non-degenerate. Thus there exists $\gamma = \{v_1 + W, \dots, v_{p+q} + W\}$ basis for V/W and $[\bar{H}]_\gamma = \begin{pmatrix} I_{p'} & 0 \\ 0 & -I_{q'} \end{pmatrix}$. From the first case p' and q' are unique. Let $\xi = \{w_1, \dots, w_k\}$ be any basis for W , by Proposition 2.5, $\beta = \{v_1, \dots, v_{p+q}, w_1, \dots, w_k\}$ is a basis for V , and it is not hard to see that

$$[H]_\beta = \begin{pmatrix} I_{p'} & 0 & 0 \\ 0 & -I_{q'} & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (83)$$

Since p' and q' are unique, it follows that the above representation is unique as well.

□

Remark. Apparently for the degenerate case you can also do the same thing in the non-degenerate case. Instead of two strict inequalities you will get one strict and the other non-strict, but that is still a contradiction. Prove me wrong please¹⁴. OMG THE TEXTBOOK USED THIS PROOF, PURBHOO PLEASE.

Corollary 4.50. *Let $A, B \in M_{n \times n}(\mathbb{R})$ be two symmetric matrices. A is congruent to B if and only if they have the same number of positive eigenvalues and same number of negative eigenvalues.*

Proof. The associated symmetric forms will have the same Sylvester's form. QED. □

What about congruence over other fields? Things get a lot more complicated. Even if we look at 2 by 2 matrices over \mathbb{Q} , the result is not so simple. For example, the identity I_2 is congruent to kI_2 if and only if $k \in \mathbb{Z}$ can be written as a sum of two squares. In general, we should consider all the extension of fields in order to make a reasonable classification.

It turns out anti-symmetric forms are nicer (kind of deep) as in that they have rather simple classifications which do not depend on the field.

¹⁴In the case my effort in writing the last part of the proof will be spiritually rewarding.

5 Tensor Algebra

Prof. Purbhoo has a much more detailed notes. This will probably never be completed. In the best scenario I can add them during winter break.