1. Review of Linear Algebra

Vaughan Sohn

October 4, 2024

Contents

Vector space and Basis

Vector space

Definition 1 (vector space)

A **vector space** is a set V along with an addition on V and a scalar multiplication on V for every $u, v \in V$, $a \in \mathbb{C}$.

- (addition) $u + v \in V$
- (scalar multiplication) $au \in V$

By definition of vector space, satisfies the following properties:

1) (commutativity) $u + v = v + u$,
2) (associativity) $(u + v) + w = u + (v + w)$ and $(ab)v = a(bv)$,
3) (additive identity) There exists an element $0 \in V$ s.t. $v + 0 = v$,
4) (additive inverse) There exists an element $w \in V$ s.t. $v + w = 0$,
5) (multiplicative identity) There exists an element s.t. $1v = v$,
6) (distributive properties) $a(u + v) = au + au$ and $(a + b)v = av + bv$.

Linear combination

Definition 2 (linear combination and span)

A **linear combination** of a list $\{|v_1\rangle, ..., |v_m\rangle\}$ of vectors in V is a vector of the form

$$|v\rangle = \sum_i a_i |v_i\rangle = a_1 |v_1\rangle + + a_m |v_m\rangle \Rightarrow \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$$

where $a_1, ..., a_m \in \mathbb{C}$. And, V is called the **span** of $\{|v_1\rangle, ..., |v_m\rangle\}$, denoted by $span(|v_1\rangle, ..., |v_m\rangle)$. In other words:

$$\text{span}(|v_1\rangle, ..., |v_m\rangle) = \{a_1 |v_1\rangle + + a_m |v_m\rangle : a_1, \ldots, a_m \in \mathbb{C}\}$$

Linearly independent

Definition 3 (linearly independent)

A list $\{|v_1\rangle, ..., |v_m\rangle\}$ of vectors in V is called **linearly independent** if the *only* choice of $a_1, ..., a_m \in \mathbb{C}$ that makes

$$a_1 |v_1\rangle + \cdots + a_m |v_m\rangle = 0$$

is $a_1 = \cdots = a_m = 0$.

Definition 4 (linearly dependent)

A list $\{|v_1\rangle, ..., |v_m\rangle\}$ of vectors in V is called **linearly dependent** if the *exists* a set of numbers $a_1, ..., a_m \in \mathbb{C}$ with $a_i \neq 0$ for at least one value of i, such that

$$a_1 |v_1\rangle + \cdots + a_m |v_m\rangle = 0.$$

Basis

Definition 5 (basis)

A **basis** of V is a list of vectors in V that is linearly *independent* and *spans* V.
The number of elements in the basis is defined to be the *dimension* of V.

- Basis가 주어지면, V에 있는 어떤 vector $|v\rangle \in V$도 basis vector들의 linear combination으로 쓸 수 있다.

$$|v\rangle = \sum_i a_i |v_i\rangle \to \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

- Example: $\mathbb{C}^2$의 basis로 사용될 수 있는 2개의 집합이 있을 때, vector $|v\rangle$를 다른 basis의 linear combination으로 나타내면?

$$|v_1\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |v_2\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|u_1\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |u_2\rangle \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Linear Operator

Linear operator

Definition 6 (linear operator)

A function from a vector space to vector space $A : V \to W$ is called an **linear map**.

$$A\left(\sum_i a_i \left|v_i\right\rangle\right) = \sum_i a_i A(\left|v_i\right\rangle)$$

Specially, operator from a vector space to *itself* is called an **linear operator**.

Theorem 7

Set of all linear operator $V \to W$ forms a vector space and denoted by:

$$\mathcal{L}(V, W)$$

$*$ Proof:

Matrix representation

- $A : V \to W$이고 각 벡터공간의 basis가 $\{|v_1\rangle, \cdots, |v_m\rangle\}$, $\{|w_1\rangle, \cdots, |w_n\rangle\}$라고 하자.
- V의 어떤 basis vector에 대해서 linear operator를 적용한 결과는 W 벡터공간안에 있는 벡터이다.

$$A |v_i\rangle \in W$$

- 따라서 이 벡터는 $\{|w_i\rangle\}$의 linear combination으로 나타낼 수 있다.

$$A |v_j\rangle = \sum_i A_{ij} |w_i\rangle$$

이때 coefficient A_{ij}를 operator A를 표현하는 matrix의 원소로 사용한다.

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nm} \end{pmatrix}$$

Inner product and Outer product

Inner product

Definition 8 (inner product)

An **inner product** is a function which takes as input two vectors $|v\rangle, |w\rangle \in V$ and produces a complex number as output.

$$(,): V \times V \to \mathbb{C}$$

Any operation can be defined as **inner product** if it satisfies

- linear in the second argument

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle \right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle),$$

- (complex conjugation) $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$,
- (non-negative integer) $(|v\rangle, |w\rangle) \geq 0$, with equality if and only if $|v\rangle = 0$.

- Note that the definition implies

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle \right) = \qquad\qquad .$$

- Inner product가 정의되는 vector space를 *inner product space*라고 한다.

Inner product

Definition 9 (norm)

We define the **norm** of a vector $|v\rangle$ by

$$\sqrt{\langle v|v\rangle} = \| \, |v\rangle \, \|.$$

If norm of a vector $|v\rangle$ is $\| \, |v\rangle \, \| = 1$, we call it as *unit vector*.

Definition 10 (orthogonality)

Vecotrs $|w\rangle$ and $|v\rangle$ are **orthogonal** if their inner product is zero.

$$\langle v|w\rangle = 0$$

Definition 11 (orthonormal)

A set of vectors is **orthonormal** if each vector is a unit vector, and each vector pairs is orthogonal.

$$\langle v|w\rangle = 0, \quad \text{and} \quad \langle v|v\rangle = 1, \langle w|w\rangle = 1$$

Outer product

Definition 12 (outer product)

An **outer product** is a linear operator which takes as input vector $|v'\rangle \in V$ and produces a vector $|\psi\rangle \in W$ as output.

$$|w\rangle \langle v| : V \to W$$

where $|w\rangle \in W, |v\rangle \in V$.

$$(|w\rangle \langle v|) |v'\rangle = |w\rangle \langle v|v'\rangle = \underbrace{\langle v|v'\rangle}_{\text{scalar}} \underbrace{|w\rangle}_{\text{vector } \in W} = |\psi\rangle$$

✓meaning: outer-product는 2개의 vector에 대해 연산하여 하나의 matrix; linear operator를 결과로 만들어낸다.

Completeness

Theorem 13 (completeness)

Any orthonormal basis $\{|i\rangle\}$ for V, an arbitrary vector $|v\rangle$ can be written as $|v\rangle = \sum_i v_i |i\rangle$ for some set of complex numbers v_i that $v_i = \langle i|v\rangle$.
Therefore, substituting into v_i,

$$|v\rangle = \sum_i \underbrace{\langle i|v\rangle}_{scalar} |i\rangle = \sum_i |i\rangle \langle i| |v\rangle$$

Since this is true for any $|v\rangle$, so we can define identity operator

$$I = \sum_i |i\rangle \langle i|$$

which is called the completeness relation.

- $A : V \to W$ 인 linear operator에 대해서, 양변에 각 vector space에 대한 identity operator를 취하면 다음의 표현을 얻을 수 있다.

$$A = I_W A I_V = \sum_{ij} |w_j\rangle \langle w_j| A |v_i\rangle \langle v_i| = \sum_{ij} \langle w_j| A |v_i\rangle |w_j\rangle \langle v_i| ,$$

- 이러한 표현을 A에 대한 outer product representation이라고 한다.
- $A_{ij} = \langle w_j|A|v_j\rangle$

Eigenvalue and Eigenvector

Eigenvalue and eigenvector

Definition 14 (eigenvalue and eigenvector)

A number λ is called an **eigenvalue** A and a non-zero vector $|v\rangle$ is called an **eigenvector** of A if there exists such that

$$A|v\rangle = \lambda|v\rangle$$

✓meaning: linear operator의 transform과 동일한 결과를 단순한 scalar multiplication으로 만들어낼 수 있는 특수한 case를 eigenvalue-vector라고 한다. 직관적으로는 linear transformation의 회전축에 대응된다고 생각할 수 있다.

- $C(\lambda) = 0$을 만족시키는 λ가 eigenvalue이다.

$$C(\lambda) = \det(A - \lambda I)$$

- Eigenvalue λ에 대한 *eigenspace*는 eigenvalue가 λ인 eigenvector들의 집합으로 V의 subspace이다.

Spectral decomposition

- 다음과 같이 vector space V에 작용하는 linear operator $A : V \to V$에 대해 eigenvalue $\{\lambda_i\}$와 orthonormal eigenbasis $\{|i\rangle\}$로 decomposition 하는 과정을 *Spectral decomposition*이라고 한다.

$$A = \sum_i \lambda_i |i\rangle \langle i|$$

- Spectral decomposition을 할 수 있는 operator는 *diagonalizable*하다고 한다.
- Example: Pauli Z matrix에 대해 spectral decomposition은

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \qquad\qquad\qquad .$$

Matrix properties: Hermitian and Unitary

Definition 15 (linear functional)

Set of all linear operator from $V \to \mathbb{C}$.

$$\mathcal{L}(V, \mathbb{C})$$

✓meaning: 벡터를 상수로 mapping시키는 operator를 linear functional이라고 한다.

Theorem 16 (Riesz representation theorem)

Suppose φ is a linear functional on vector space V. Then there is a unique vector $u \in V$ s.t.

$$\varphi |v\rangle = \langle u|v\rangle$$

✓meaning: 내적이 linear functional의 연산 결과와 동일한 벡터가 존재한다.

Corollary 17

Suppose $A : V \to V$ is a linear operator on vector space V. By Riesz Representation Theorem, there is a unique operator $B \equiv A^\dagger$ for all vectors $|v\rangle, |w\rangle \in V$, s.t.

$$(|v\rangle, A|w\rangle) = (B|v\rangle, |w\rangle)$$

$$\langle v|A|w\rangle = \langle v|B^\dagger|w\rangle = \langle v|(A^\dagger)^\dagger|w\rangle$$

$*$ Proof:

Hermitian, normal and unitary

Definition 18 (hermitian)

Operator A is the **Hermitian** operator such that

$$A^\dagger = A.$$

Corollary 19 (projector)

Operator P is the **projector** *onto the subspace W.Where W has orthonormal basis $\{|1\rangle, \cdots |k\rangle\}$ construct from orthonormal basis $\{|1\rangle, \cdots, |d\rangle\}$for V.*

$$P \equiv \sum_{i=1}^{k} |i\rangle \langle i|$$

- Projector가 $|v\rangle \in V$에 대해 취하는 연산은 다음과 같다. 즉, 일부 basis만 사용한 linear combination으로 만들어지는 벡터이다.

$$P|v\rangle = \sum_{i=1}^{k} |i\rangle \langle i|v\rangle = \sum_{i=1}^{k} v_i |i\rangle$$

- $|v\rangle \in V$는 P에 대해 $|v\rangle = P|v\rangle + (I - P)|v\rangle$로 나눌 수 있다.
- P는 Hermitian operator이다. (i.e., $P^\dagger = P$)

Hermitian, normal and unitary

Definition 20 (normal)

Operator A is the **normal** operator such that

$$AA^\dagger = A^\dagger A.$$

- Hermitian operator는 normal operator이다. $\rightarrow$ Hermitian has spectral decomposition
- Normal operator는 *if and only if* real eigenvalues만 가질 때, Hermitian 이다.
- Vector space V에 대한 Normal operator는 V에 대한 some orthonormal basis를 사용하여 diagonal 할 수 있다. $\rightarrow$ normal has spectral decomposition

Definition 21 (positive operator)

Operator A is positive operator such that for some operator B

$$A = B^\dagger B.$$

Condition of positive operator:

- (hermitian) $A = A^\dagger$ $(*)$
- (positive semi-definite) $\langle v|A|v\rangle \geq 0$

Hermitian, normal and unitary

Definition 22 (Unitary)

Operator U is **unitary** operator such that

$$UU^\dagger = U^\dagger U = I.$$

In other words,

$$U^\dagger = U^{-1}.$$

- Unitary operator는 normal operator이다. $\rightarrow$ unitary has spectral decomposition
- Unitary operator는 inner products 결과를 보존한다. $(*)$

$$(U|v\rangle, U|w\rangle) = \langle v|w\rangle$$

- 만약 U가 orthonormal basis $\{|v_i\rangle\}$에 취해지면, unitary operator의 성질로 인해$(*)$ 내적 결과로 만들어지는 벡터들의 집합 $\{|w_i\rangle\}$도 orthonormal basis가 된다. 따라서 unitary operator는 다음과 같이 표현할 수 있다.

$$U = \sum_i |w_i\rangle \langle v_i|,$$

where $|w_i\rangle = U|v_i\rangle$.

Tensor product

Definition 23 (tensor product)

Suppose V and W be vector spaces with respective bases $\{|i\rangle\}$ and $\{|j\rangle\}\}$. The tensor product of these two vector spaces is defined as

$$V \otimes W, \quad \{|i\rangle \otimes |j\rangle\} \in V \otimes W.$$

✓meaning: Tensor product로 만들어지는 벡터는 두 vector space V, W의 basis vector$|i\rangle$, $|j\rangle$들의 tensor product의 linear combination으로 표현된다. 즉, 결과 벡터는 $|i\rangle \otimes |j\rangle$를 basis로 갖는 새로운 vector space에 존재한다.

$$|v\rangle \otimes |w\rangle = \sum_{i,j} \alpha_{ij} |i\rangle \otimes |j\rangle$$

By definition of tensor product, satisfies the following properties:
For an arbitrary scalar z and vectors $|v\rangle \in V$ and $|w\rangle \in W$

1) $z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$,
2) $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes w$,
3) $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

Tensor product for Operators

Definition 24 (tensor product for operators)

Combine linear operator $A : V \to V'$ and $B : W \to W'$, then we define the **tensor product linear operator** $C : V \otimes W \to V' \otimes W'$ as

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle$$

more general,

$$C = \sum_i c_i A_i \otimes B_i.$$

- Example : The tensor product of the Pauli matrices X and Y is

$$X \otimes Y =$$

Useful concepts: projector, trace and commutator

Definition 25 (operator function)

Let $A = \sum_a a |a\rangle \langle a|$ be a spectral decomposition for a normal operator A. Then we define **operator function** as

$$f(A) = \sum_a f(a) |a\rangle \langle a| .$$

✓meaning: operator의 spectral decomposition에 대해 eigenvalue에만 적용된다.

- Example: $A = Z, f(x) = e^{\theta x}$ then,

$$f(Z) =$$

Trace

Definition 26 (trace)

$$\text{tr}(A) = \sum_i A_{ii} = \sum_i \langle i|A|i\rangle$$

By definition of trace, satisfies the following properties:

- $\text{tr}(AB) = \text{tr}(BA)$
- $\text{tr}(A+B) = \text{tr}(A) + \text{tr}(B)$
- $\text{tr}(zA) = z \cdot \text{tr}(A)$
- (unitary invariant)
$$\text{tr}(UAU^\dagger) = \text{tr}(A)$$
- $\langle\psi|A|\psi\rangle = \text{tr}[A\,|\psi\rangle\,\langle\psi|]$ ($*$)

$*$ Proof:

Commutator

Definition 27 (commutator)

A, B is linear operator,
commutator:

$$[A, B] = AB - BA$$

anti-commutator:

$$\{A, B\} = AB + BA$$

Theorem 28

If commutator is zero; $[A, B] = 0$ *then if and only if there exists an orthogonal basis that diagonalizable* A *and* B **simultaneously**.

Decompositions

Polar decomposition

Let A be a linear operator on a vector space V. Then there exists *unitary* U and *positive operators* J and K such that

$$A = UJ = KU$$

- If A is invertible, then U is unique. (i.e., If A is full rank.)
- J, K가 positive operator 이므로 다음과 같다.

$$J = \sqrt{A^\dagger A}, \qquad K = \sqrt{AA^\dagger}.$$

- A는 square matrix가 아니어도 된다.

Singular value decomposition

Let A be a linear operator on a vector space V. Then there exists unitary U and V and a diagonal matrix D with nonnegative entries such that

$$A = UDV.$$

$*$ Proof: (hint: using polar decomposition)

Shmidt decomposition

Suppose we have a vector in a composite system $V \otimes W$. Then there exist orthonormal basis in V and W such that

$$|a\rangle = \sum_i \lambda_i \, |v_i\rangle \otimes |w_i\rangle$$

$*$ Proof: (hint: using singular value decomposition)

References

- Sheldon Axler, Linear Algebra Done Right, 3th
- Lecture notes for QU511: Quantum Computing (Fall 2024)