Quantum Computing

Lecture on Linear Algebra

Sources: Angela Antoniu, Bulitko, Rezania, Chuang, Nielsen

Introduction to Quantum Mechanics

- **Review Chapters 1 and 2 from Chuang and Nielsen**
- **Objective**
  - To introduce all of the fundamental principles of Quantum mechanics
- **Quantum mechanics**
  - The most realistic known description of the world
  - The basis for quantum computing and quantum information
- **Why Linear Algebra?**
  - LA is the prerequisite for understanding Quantum Mechanics
- **What is Linear Algebra?**
  - … is the study of vector spaces… and of
  - linear operations on those vector spaces

Linear algebra -Lecture objectives

- Review basic concepts from Linear Algebra:
  - Complex numbers
  - Vector Spaces and Vector Subspaces
  - Linear Independence and Bases Vectors
  - Linear Operators
  - Pauli matrices
  - Inner (dot) product, outer product, tensor product
  - Eigenvalues, eigenvectors, Singular Value Decomposition (SVD)
- Describe the standard notations (the Dirac notations) adopted for these concepts in the study of Quantum mechanics
- … which, in the next lecture, will allow us to study the main topic of the Chapter: the postulates of quantum mechanics

Review: The Complex Number System

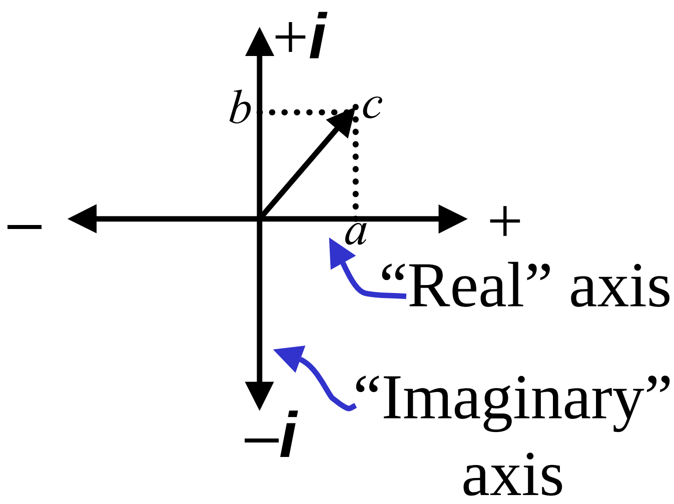
- It is the extension of the real number system via closure under exponentiation.

$$\boldsymbol{i} \equiv \sqrt{-1} \qquad c = a + b\boldsymbol{i} \qquad (c \in \mathbf{C},\ a, b \in \mathbf{R})$$

The "imaginary" unit

$$\mathrm{Re}\ [c] \equiv a$$

$$\mathrm{Im}\ [c] \equiv b$$



- *(Complex) conjugate:*

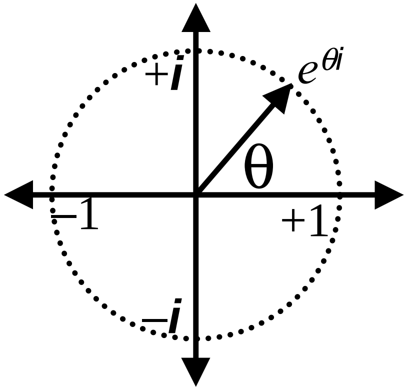
$$c^* = (a + b\boldsymbol{i})^* \equiv (a - b\boldsymbol{i})$$

- *Magnitude* or *absolute value*:

$$|c|^2 = c^*c = a^2 + b^2$$

$$|c| \equiv \sqrt{c^* c} = \sqrt{(a - b\boldsymbol{i})(a + b\boldsymbol{i})} = \sqrt{a^2 + b^2}$$

Review: Complex Exponentiation



- Powers of *i* are complex units:

$$e^{\theta i} \equiv \cos\theta + i\sin\theta$$

- Note:

$$e^{\pi i/2} = i$$

$$e^{\pi i} = -1$$

$$e^{3\pi i/2} = -i$$

$$e^{2\pi i} = e^{0} = 1$$

Recall: What is a qubit?

- A qubit has two possible states $|0\rangle \text{ or } |1\rangle$
- Unlike bits, a quibit can be in a **state other than**

$$|0\rangle \text{ or } |1\rangle$$

- We can form linear combinations of states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- A quibit state is a unit vector in a two dimensional ***complex*** *vector space*

Properties of Qubits

- Qubits are computational basis states

  - orthonormal basis

$$\langle i | j \rangle = \delta_{ij} \qquad \delta_{ij} = \begin{cases} 0 \text{ for } i \neq j \\ 1 \text{ for } i = j \end{cases}$$

  - we <u>cannot</u> examine a qubit to determine its quantum state

    - A measurement yields

0 with probability $|\alpha|^2$ 1 with probability $|\beta|^2$

where $|\alpha|^2 + |\beta|^2 = 1$

Complex numbers

- A complex number $z_n \in C$ is of the form $a_n, b_n \in R$ where $z_n = a_n + ib_n$ **and i^2=-1**
- Polar representation

  $z_n = u_n e^{i\theta_n}$, where $u_n, \theta_n \in R$

  - *With* $u_n = \sqrt{a_n^2 + b_n^2}$ *the modulus or magnitude*
  - *And the phase* $\theta_n = \arctan\left(b_n / a_n \right)$

- *Complex* ***conjugate***

$z_n = u_n(\cos\theta_n + i\sin\theta_n)$ $z_n^* = (a_n + ib_n)^* = a_n - ib_n$

(Abstract) Vector Spaces

- A concept from linear algebra.
- A vector space, in the abstract, is any set of objects that can be combined like vectors, *i.e.*:
  - you can add them
    - addition is associative & commutative
    - identity law holds for addition to zero vector **0**
  - you can multiply them by scalars (incl. –1)
    - associative, commutative, and distributive laws hold
- **Note**: There is no *inherent* basis (set of axes)
  - the vectors *themselves* are the fundamental objects
  - rather than being just lists of coordinates

Hilbert spaces

- A *Hilbert space* is a vector space in which the scalars are complex numbers, with an *inner product* (dot product) operation $\bullet : H \times H \rightarrow \mathbf{C}$
  - Definition of inner product:

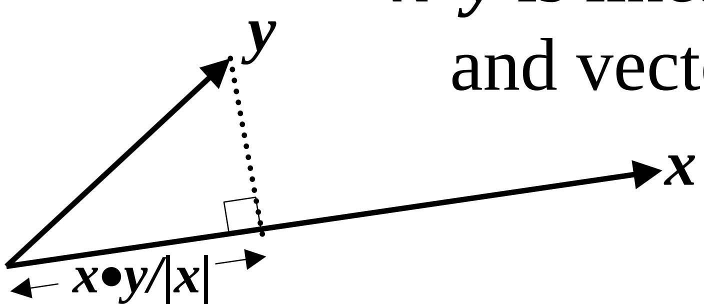
$\boldsymbol{x}\bullet\boldsymbol{y} = (\boldsymbol{y}\bullet\boldsymbol{x})^*$ (* = complex conjugate)

$\boldsymbol{x}\bullet\boldsymbol{x} \geq 0$

$\boldsymbol{x}\bullet\boldsymbol{x} = 0$ if and only if $\boldsymbol{x} = \mathbf{0}$

$\boldsymbol{x}\bullet\boldsymbol{y}$ is linear, under scalar multiplication and vector addition within both $\boldsymbol{x}$ and $\boldsymbol{y}$

"Component" picture:



Another notation often used:

$$\boldsymbol{x}\bullet\boldsymbol{y} \equiv \langle \boldsymbol{x} | \boldsymbol{y} \rangle$$

"bracket"

Vector Representation of States

- Let $S=\{s_0, s_1, \ldots\}$ be a maximal set of distinguishable states, indexed by i.
- The basis vector $\boldsymbol{v}_i$ identified with the i^{th} such state can be represented as a list of numbers:

$$\begin{array}{l} \quad\quad\quad s_0\ s_1\ s_2 \quad\quad s_{i\text{-}1}\ s_i\ s_{i+1} \\ \boldsymbol{v}_i = (0,\ 0,\ 0,\ \ldots,\ 0,\ 1,\ 0,\ \ldots\ ) \end{array}$$

- Arbitrary vectors $\boldsymbol{v}$ in the Hilbert space can then be defined by linear combinations of the $\boldsymbol{v}_i$:

$$\boldsymbol{v} = \sum_i c_i \boldsymbol{v}_i = (c_0, c_1, \ldots)$$

- And the inner product is given by:

$$\langle \boldsymbol{x} | \boldsymbol{y} \rangle = \sum_i x_i^* y_i$$

Dirac's Ket Notation

- Note: The inner product definition is the same as the matrix product of $\boldsymbol{x}$, as a conjugated row vector, times $\boldsymbol{y}$, as a normal column vector.

$$\langle \boldsymbol{x} | \boldsymbol{y} \rangle = \sum_i x_i^* y_i$$

"Bracket"

$$= \begin{bmatrix} x_1^* & x_2^* & \cdots \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \end{bmatrix}$$

- This leads to the definition, for state s, of:
  - The "bra" $\langle s|$ means the row matrix $[c_0^* \; c_1^* \; \ldots]$
  - The "ket" $|s\rangle$ means the column matrix $\rightarrow$ $\begin{bmatrix} c_1 \\ c_2 \\ \vdots \end{bmatrix}$
- The adjoint operator † takes any matrix $\boldsymbol{M}$ to its conjugate transpose $\boldsymbol{M}^\dagger \equiv \boldsymbol{M}^{\mathrm{T}*}$, so $\langle s|$ can be defined as $|s\rangle^\dagger$, and $\boldsymbol{x} \bullet \boldsymbol{y} = \boldsymbol{x}^\dagger \boldsymbol{y}$.

Vectors

- Characteristics:
  - Modulus (or magnitude)
  - Orientation
- Matrix representation of a vector

$$|\mathbf{v}\rangle = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \text{ (a column), and its dual}$$

$$|\mathbf{v}\rangle^{\tau} = \langle \mathbf{v}| = [z_1^*, \cdots, z_n^*] \text{ (row vector)}$$

Vector Space, definition:

- A vector space (of dimension ***n***) is a set of ***n*** vectors satisfying the following axioms (rules):
  - **Addition:** add any two vectors $|\mathbf{v}\rangle$ and $|\mathbf{v}'\rangle$ pertaining to a vector space, say $\mathbf{C}^n$, obtain a vector,

$$|\mathbf{v}\rangle + |\mathbf{v}'\rangle = \begin{bmatrix} z_1 + z_1' \\ \vdots \\ z_n + z_n' \end{bmatrix}$$

the sum, with the properties :

    - Commutative: $|\mathbf{v}\rangle + |\mathbf{v}'\rangle = |\mathbf{v}'\rangle + |\mathbf{v}\rangle$
    - Associative: $(|\mathbf{v}\rangle + |\mathbf{v}'\rangle) + |\mathbf{v}''\rangle = |\mathbf{v}\rangle + (|\mathbf{v}'\rangle + |\mathbf{v}''\rangle)$
    - Any $|\mathbf{v}\rangle$ has a zero vector (called the origin):
    - To every $|\mathbf{v}\rangle$ in $\mathbf{C}^n$ corresponds a unique vector - $|\mathbf{v}\rangle$ such as $|\mathbf{v}\rangle + \mathbf{0} = |\mathbf{v}\rangle$

$$|\mathbf{v}\rangle + (-|\mathbf{v}\rangle) = \mathbf{0}$$

  - Scalar **multiplication: → next slide**

Vector Space (cont)

- *Scalar* ***multiplication: for any scalar***

$z \in C$ and vector $|\mathrm{v}\rangle \in C^n$ there is a vector

$z|\mathbf{v}\rangle = \begin{bmatrix} zz_1 \\ \vdots \\ zz_n \end{bmatrix}$, the scalar product, in such way that $1|\mathbf{v}\rangle = |\mathbf{v}\rangle$

- **Multiplication by scalars is Associative:**
- $$z(z'|\mathbf{v}\rangle) = (zz')|\mathbf{v}\rangle$$

distributive with respect to vector addition:

$$z(|\mathbf{v}\rangle + |\mathbf{v}'\rangle) = z|\mathbf{v}\rangle + z|\mathbf{v}'\rangle$$

- **Multiplication by vectors is**

distributive with respect to scalar addition: $(z+z')|\mathbf{v}\rangle = z|\mathbf{v}\rangle + z'|\mathbf{v}\rangle$

- **A Vector subspace in an n-dimensional vector space is a non-empty subset of vectors satisfying the same axioms**

Basis vectors

- Or SPANNING SET for C^n: any set of n vectors such that any vector in the vector space C^n can be written using the n base vectors

- Example for C^2 (n=2):

$$|0\rangle \text{ corresponds to } \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle \text{ corresponds to } \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \text{ corresponds to } \alpha_0\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

which is a linear combination of the 2 dimensional basis vectors $|0\rangle$ and $|1\rangle$

Bases and Linear Independence

Spanning set: a set of vectors such that any vector in the space can be written as a linear combination of vectors in the set

$$\{|v_1\rangle, \ldots, |v_n\rangle\} \longrightarrow |v\rangle = \sum_{j=1}^{n} a_j |v_j\rangle \quad \text{for any } |v\rangle$$

Linear independence: a set of vectors is linearly independent if there is no linear combination of them which adds to zero non-trivially

$$\sum_{j=1}^{n} a_j |v_j\rangle = 0 \quad \text{iff every } a_j = 0$$

Basis: a linearly independent spanning set **Always exists!**

Quantum Notation

(Sometimes denoted by bold fonts)

z^*	Complex conjugate of z
$\vert\psi\rangle$	Vector (a ket) -- this will represent a possible state of the discrete quantum system
$\langle\psi\vert$	Vector dual to $\vert\psi\rangle$ (a bra)
$\langle\psi\vert\varphi\rangle$	Inner product of two vectors
$\vert\psi\rangle\otimes\vert\varphi\rangle$	Tensor product of two vectors
$\mathbf{A}$	A matrix -- this will represent an operator which can modify a quantum state
$\langle\psi\vert\mathbf{A}\vert\varphi\rangle$	Inner product of $\vert\psi\rangle$ and $\mathbf{A}\vert\varphi\rangle$

(Sometimes called Kronecker multiplication)

Linear Operators

Physical operations on quantum states are represented by linear operators which act on the states

Linear operator: An operator which maps one vector space into another that is linear in its arguments is called a linear operator

$$\mathbf{A}\left(\sum_{j=1}^{n} a_j |v_j\rangle\right) = \sum_{j=1}^{n} a_j \mathbf{A}(|v_j\rangle)$$

Linear operators ⟷ matrices (matrix elements determined by specifying action on a basis)

Basis for V   Basis for W

$$\mathbf{A}(|v_i\rangle) = \sum_j A_{ij} |w_j\rangle$$

Pauli Matrices

A useful set of matrices which acts on a 2-dimensional vector space are the Pauli matrices:

X is like inverter

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- **Properties: Unitary** $(\boldsymbol{\sigma}_k)^{\tau}\boldsymbol{\sigma}_k = \mathbf{I}, \forall k$

  and Hermitian $(\boldsymbol{\sigma}_k)^{\tau} = \boldsymbol{\sigma}_k$

Inner Products

Inner Product: A method for combining two vectors which yields a complex number $\left(|\psi\rangle, |\varphi\rangle\right) \equiv \langle\psi|\varphi\rangle \mapsto \mathrm{C}$ that obeys the following rules

- $(\ ,\ )$ is linear in its 2nd argument

$$\left(|v\rangle, \sum_k a_k |w_k\rangle\right) = \sum_k a_k \left(|v\rangle, |w_k\rangle\right)$$

- $\left(|v\rangle, |w\rangle\right) = \left(|w\rangle, |v\rangle\right)^*$

- $\left(|v\rangle, |v\rangle\right) \geq 0$

Example: C^n

$$\left((w_1, \ldots, w_n), (z_1, \ldots, z_n)\right) = w_1^* z_1 + \cdots w_n^* z_n$$

Eigenvalues and Eigenvectors

More on Inner Products

Hilbert Space: the inner product space of a quantum system

Orthogonality: $|w\rangle$ and $|v\rangle$ are orthogonal if $\langle v|w\rangle = 0$

Norm: $\||v\rangle\| \equiv \sqrt{\langle v|v\rangle}$ Unit: $\frac{|v\rangle}{\sqrt{\langle v|v\rangle}}$ is the unit vector parallel to $|v\rangle$

Orthonormal basis: : a basis set $\{|v_1\rangle, \ldots, |v_n\rangle\}$ where $\langle v_i|v_j\rangle = \delta_{ij}$

Gram-Schmidt Orthogonalization: an algorithmic procedure for finding an orthonormal basis $|j\rangle$ from a given basis

$$\left.\begin{aligned} |v\rangle &= \sum_{j=1}^{n} v_j |j\rangle \\ |w\rangle &= \sum_{j=1}^{n} w_j |j\rangle \end{aligned}\right\} \Longrightarrow \langle v|w\rangle = \sum_j v_j^* w_j$$

(inner product of 2 vectors is equal to inner product of the matrix reps of the 2 vectors)

Outer Products

Let $|w\rangle$ be a vector in the vector space W

Let $|v\rangle$ be a vector in the vector space V

Outer product: $|w\rangle\langle v|$ is the outer product of $|w\rangle$ and $|v\rangle$

It is a linear map from V into W defined by

$$|w\rangle\langle v|\left(|v'\rangle\right)=|w\rangle\langle v|v'\rangle$$

Completeness relation: Let $|j\rangle$ be a basis for V. It is easy to show that

$$\sum_j |j\rangle\langle j| = \mathbf{I}$$

$$\text{i.e.} \sum |j\rangle\langle j|\left(|v\rangle\right)=|v\rangle \text{ for every } |v\rangle$$

Eigenvalues and Eigenvectors

$$\mathbf{A}|v\rangle = \lambda_v|v\rangle = v|v\rangle$$

Eigenvalue

Eigenvector

obtain by finding all roots to the eqn

$$\det(\mathbf{A}-\lambda\mathbf{I})=0$$

Diagonalizable: A matrix $\mathbf{A}$ is diagonalizable if it can be written as $\mathbf{A}=\sum_j \lambda_j |j\rangle\langle j|$ ← orthonormal basis

e.g. $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=|0\rangle\langle 0|-|1\rangle\langle 1|$

Degeneracy: when two (or more) eigenvalues are equal

In this case the eigenspace is larger than one dimension

Hermitian Operators

Adjoint: $\mathbf{A}^{\tau}$ is the adjoint of $\mathbf{A}$ if $\left(\mathbf{A}^{\tau}|v\rangle, |w\rangle\right) = \left(|v\rangle, \mathbf{A}|w\rangle\right)$ for all vectors $|v\rangle, |w\rangle$ in the vector space V

Properties: $\mathbf{A}^{\tau} = \mathbf{A}^{*T}$ $\quad \left(\mathbf{A}^{\tau}\right)^{\tau} = \mathbf{A}$ $\quad \left(\mathbf{AB}\right)^{\tau} = \mathbf{B}^{\tau}\mathbf{A}^{\tau}$

$$|v\rangle^{\tau} = \langle v|$$

Hermiticity: $\mathbf{A}$ is Hermitian if $\mathbf{A}^{\tau} = \mathbf{A}$

e.g. $\mathbf{P} = \sum_{j=1}^{k} |j\rangle\langle j|$ Projects any vector into a k-dim'l subspace

Normal: $\mathbf{A}$ is Normal if $\mathbf{A}^{\tau}\mathbf{A} = \mathbf{A}\mathbf{A}^{\tau}$

can show: Normal $\longleftrightarrow$ Diagonalizable (spectral decomposition)

Unitary and Positive Operators

Unitary: $\mathbf{U}$ is unitary if $\mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$

can write: $\mathbf{U} = \sum_j |\hat{j}\rangle\langle j|$ where $|j\rangle$ and $|\hat{j}\rangle$ are any two distinct orthonormal bases for the vector space V, such that $\mathbf{U}|j\rangle = |\hat{j}\rangle$

Note:

$$(\mathbf{U}|v\rangle, \mathbf{U}|w\rangle) = \langle v|\mathbf{U}^\dagger\mathbf{U}|w\rangle = \langle v|w\rangle = (|v\rangle, |w\rangle)$$ (preserves inner product)

Positive: $\mathbf{B}$ is positive if $(|v\rangle, \mathbf{B}|v\rangle) \geq 0$ for every $|v\rangle$ in V (no negative eigenvalues!)

If $(|v\rangle, \mathbf{B}|v\rangle) > 0$ for every $|v\rangle$ in V ➡ $\mathbf{B}$ is positive definite (all positive eigenvalues!)

Tensor Products

A tensor product is a larger vector space formed from two smaller ones simply by combining elements from each in all possible ways that preserve both linearity and scalar multiplication

If V is a vector space of dimension n $|v\rangle$
& W is a vector space of dimension m $|w\rangle$
then V⊗W is a vector space of dimension mn $|v\rangle \otimes |w\rangle$

e.g.

$|0\rangle \otimes |0\rangle = |00\rangle$ $|1\rangle \otimes |1\rangle = |11\rangle$ are elements of V⊗V

and so is $|00\rangle + |11\rangle$ → qualitatively new feature: entangled states!

More on Tensor Products

$$z\left(|v\rangle \otimes |w\rangle\right) = \left(z|v\rangle \otimes |w\rangle\right) = \left(|v\rangle \otimes z|w\rangle\right)$$

scalar multiplication

$$|v\rangle \otimes \left(|w_1\rangle + |w_2\rangle\right) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

$$\left(|v_1\rangle + |v_2\rangle\right) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

linearity

$\mathbf{A}$ acts on $|v\rangle$ $\quad$ $\mathbf{B}$ acts on $|w\rangle$

$$(\mathbf{A} \otimes \mathbf{B})\left(|v\rangle \otimes |w\rangle\right) = \mathbf{A}|v\rangle \otimes \mathbf{B}|w\rangle$$

tensor product of operators

e.g.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$X \otimes Y = \begin{bmatrix} 0 \bullet Y & 1 \bullet Y \\ 1 \bullet Y & 0 \bullet Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$$

Functions of Operators

Can define the function of an operator from its power series:

$$f(x) = \sum_n a_n x^n \Rightarrow f(\mathbf{A}) = \sum_n a_n \mathbf{A}^n$$

e.g. $$\exp(\theta X) = I + \theta X + \frac{1}{2!}(\theta X)^2 + \frac{1}{3!}(\theta X)^3 + \cdots$$

$$= I + \frac{1}{2!}\theta^2 I + \cdots + \left(\theta + \frac{1}{3!}\theta^3 + \cdots\right)X$$

$$= I\cos\theta + X\sin\theta$$

For normal operators, can go beyond this using their spectral decomposition:

$$\mathbf{A} = \sum_j \lambda_j |j\rangle\langle j| \Rightarrow f(\mathbf{A}) = \sum_j f(\lambda_j)|j\rangle\langle j|$$

Trace and Commutator

Trace: $\mathrm{tr}(\mathbf{A}) = \sum_i A_{ii}$ (sum over the diagonal elements)

$$\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA}) \qquad \mathrm{tr}(z\mathbf{A} + \mathbf{B}) = z\,\mathrm{tr}(\mathbf{A}) + \mathrm{tr}(\mathbf{B})$$

Commutator: $[\mathbf{A}, \mathbf{B}] \equiv \mathbf{AB} - \mathbf{BA}$

Anti-commutator: $\{\mathbf{A}, \mathbf{B}\} \equiv \mathbf{AB} + \mathbf{BA}$

Simultaneous Diagonalization: Two Hermitian operators $\mathbf{A}$ and $\mathbf{B}$ are diagonalizable in the same basis if and only if $[\mathbf{A}, \mathbf{B}] = 0$

Polar Decomposition

For any linear operator acting on a vector space we can write

$$\mathbf{A} = \mathbf{U}\sqrt{\mathbf{A}^{\tau}\mathbf{A}}$$ (left polar decomposition)

where $\mathbf{U}$ is a unitary matrix -- it is unique if $\mathbf{A}$ has an inverse

Alternatively $$\mathbf{A} = \sqrt{\mathbf{A}\mathbf{A}^{\tau}}\,\mathbf{U}'$$ (right polar decomposition)

Singular-value decomposition:

For all square matrices, can write $\mathbf{A} = \mathbf{U}\mathbf{D}\mathbf{U}'$
where $\mathbf{D}$ is a diagonal matrix

Bibliography & acknowledgements

- Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, UK, 2002
- R. Mann,M.Mosca, Introduction to Quantum Computation, Lecture series, Univ. Waterloo, 2000 http://cacr.math.uwaterloo.ca/~mmosca/quantumcoursef00.htm
- Paul Halmos, Finite-Dimensional Vector Spaces, Springer Verlag, New York, 1974