**An Invitation to**
**Quantum Information and Quantum Computing**

- Course website:

  https://cklixx.people.wm.edu/teaching/QC-invitation.html

- Teaching Team.


* Ray-Kuang Lee, National Tsinghua University.

E-mail: rklee@ee.nthu.edu.tw. http://mx.nthu.edu.tw/~rklee/

* Chi-Kwong Li, College of William & Mary; IQC, U. of Waterloo. (李志光)

E-mail: qc1979.ckli@gmail.com, http://cklixx.people.wm.edu

* Anandu Kalleri Madhu, National Tsinghua University.

E-mail: anandu.k.madhu@gmail.com

**Objectives**

- Give a gentle introduction to quantum information and quantum computing using **elementary linear approach** and some **selected topics**.
- Hopefully, you will get a general idea how to use quantum approach with the Hilbert space (linear algebra) formalism to study and do research in

  * quantum information, quantum computing, and

  * related problems (biology, AI, image processing, etc.)

**Textbook, lecture notes, discussion, etc.**

- Nakahara and Ohmi, Quantum computing: From Linear Algebra to Physical Realizations, CRC Press, Taylor and Francis Group, New York, 2008.
- Supplementary notes and class notes will be posted on course websites.
- Discussions could be put on the chat, or sent to qc1979.ckli@gmail.com.

## Chapter 1 Basic Linear Algebra

- In this chapter, we will present the basic matrix theory tools needed in our discussion.

- In fact, "Matrix Mechanics" was a formulation of quantum mechanics by Werner Heisenberg, Max Born, and Pascual Jordan (1925).

- John von Neumann formalized the mathematical framework, and used the Hilbert space approach to understand some basic quantum phenomena.

- I will use a "pseudo quantum mechanical" approach to describe the relevant linear algebra concepts and physics notation at the beginning before we introduce the postulates of quantum mechanics.

## §1.1 Vectors

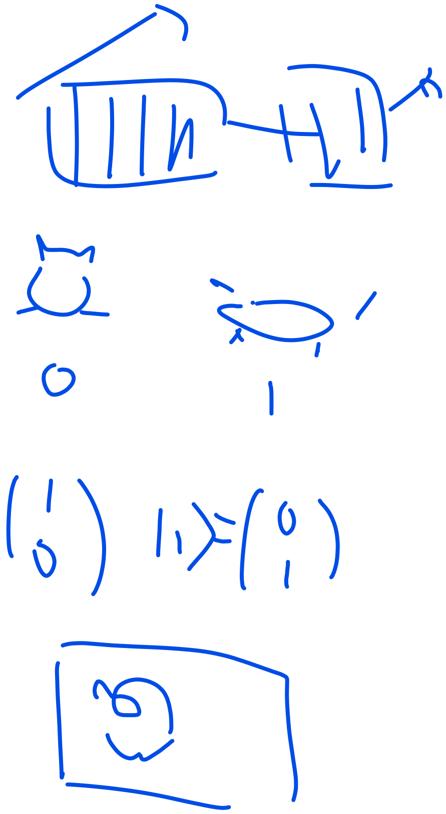
- Consider a photon, which has two (classical) states: vertical and horizontal polarization.
- One may think about the Schrödinger cat, which is either alive and dead in the physical world.
- Simple mathematical model would use

  0 and 1 to represent the two states.
- In quantum physics, we use the unit vectors

  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ to represent the states.
- A photon in a quantum environment has the form

  $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ with $a, b \in \mathbb{C}$ such that $|a|^2 + |b|^2 = 1$.

  **Note that we have to use complex numbers!**



- In general, we use complex $n \times 1$ column vectors (of length 1) to represent a quantum state with $n$ physical states.

- $\mathbb{C}^n$ is a vector space under addition and scalar multiplication.

- We use the Dirac notation, a column vector $|u\rangle \in \mathbb{C}^n$ is called a ket-vector and $\langle u|$ is the corresponding bra-vector, which is row vector equal to the conjugate transpose of $|u\rangle$.

  Example. Consider $|u\rangle = \frac{1}{5}\begin{pmatrix} 4 \\ 3i \end{pmatrix} \in \mathbb{C}^2$.

  Then $\langle u| = \frac{1}{5}(4, -3i)$.

- Quantum (vector) states are represented by unit vectors:

$$|u\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \qquad \sum_{j=1}^{n} |u_j|^2 = 1.$$

**Linear independent vectors and basis**

- Linearly independent/dependent vectors.

  A set of vectors $\{|v_1\rangle, \ldots, |v_m\rangle\}$ is linearly independent if the linear combination

  $$c_1|v_1\rangle + \cdots + c_m|v_m\rangle$$

  equals to the zero vector $|\mathbf{0}\rangle$ can only happen when

  $$(c_1, \ldots, c_m) = (0, \ldots, 0).$$

  Else, it is linear dependent.

- Linear independence can be checked by studying the homogeneous system of linear equations

  $$A|x\rangle = |\mathbf{0}\rangle \quad \text{with} \quad A = [|v_1\rangle \cdots |v_m\rangle].$$

**Basis and dimensions**

- A basis $\mathcal{B}$ for a vector space $\mathbf{V}$ is a linearly independent generating set.
- That is, a set of linearly independent set such that every vector in $\mathbf{V}$ can be written as a linear combination of vectors in $\mathcal{B}$.
- There are different basis for $\mathbf{V}$, but their sizes (cardinalities) are the same. The size of the basis is the dimension of $\mathbf{V}$.
- In $\mathbb{C}^n$, any linearly independent set or any generating set with $n$ vectors is a basis.
- One may check the matrix with these vectors as columns is invertible.

**Inner product**

- The inner product of $|u\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ in $\mathbb{C}^n$ is

$$\langle u|v\rangle = \sum_{j=1}^{n} u_j^* v_j.$$

For any $a, b \in \mathbb{C}, |u\rangle, |v\rangle \in \mathbb{C}^n$,

(1) $\langle u|av_1 + bv_2\rangle = a\langle u|v_1\rangle + b\langle u|v_2\rangle$,

(2) $\langle u, v\rangle = \langle v|u\rangle^*$

(3) $\langle \mathbf{0}|\mathbf{0}\rangle = 0$, and $\langle u, u\rangle > 0$ if $|u\rangle \neq 0$.

- The (inner product) norm of $|u\rangle$ is $\||u\rangle\| = \langle u|u\rangle^{1/2}$.

- Two vectors $|u\rangle, |v\rangle$ are orthogonal if $\langle u|v\rangle = 0$.

  Equivalently, $\langle v|u\rangle = 0$.

- A set $\{|u_1\rangle, \ldots, |u_k\rangle\} \subseteq \mathbb{C}^n$ is orthogonal if

  $\langle u_i|u_j\rangle = 0$ whenever $i \neq j$.

  If in addition, $\langle u_j|u_j\rangle = 1$, the set is orthonormal.

**Orthonormal basis**

- It is easy to check $\{|x_1\rangle, \ldots, |x_k\rangle\} \subseteq \mathbb{C}^n$ is an orthogonal/orthonormal set, namely, the $n \times k$ matrix $X = [|x_1\rangle \cdots |x_k\rangle]$ satisfies $X^\dagger X = I_k$ because the $(r, s)$ entry of $X^\dagger X$ is $\langle x_r | x_s \rangle$.

- It is easy to express a vector $|v\rangle$ as a linear combination of orthonormal basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$, namely, $|v\rangle = \sum_{j=1}^n c_j |e_j\rangle$ with $c_j = \langle e_j | v \rangle$ for $j = 1, \ldots, n$.

- The set $\{P_j = |e_j\rangle\langle e_j| : j = 1, \ldots, n\}$ forms a complete set of projection operators/matrices.

  (i) $P_j^2 = P_j$, (ii) $P_j P_k = 0$ for $j \neq k$, (iii) $P_1 + \cdots + P_n = I_n$

**Gram-Schmidt orthonormalization process**

Let $\{|x_1\rangle, \ldots, |x_m\rangle\}$ be linearly independent.

We can use the following Gram-Schmidt process to construct an orthonormal set $\{|e_1\rangle, \ldots, |e_m\rangle\}$ such that

$$\text{span}\{|x_1\rangle, \ldots, |x_\ell\rangle\} = \text{span}\{|e_1\rangle, \ldots, |e_\ell\rangle\},$$

for all $\ell = 1, \ldots, m$.

Set $|e_1\rangle = |x_1\rangle / \| |x_1\rangle \|$.

For $k > 1$, set $|f_k\rangle / \| |f_k\rangle \|$, where

$$|f_k\rangle = |x_k\rangle - a_1|e_1\rangle - \cdots - a_{k-1}|e_{k-1}\rangle$$

with $a_j = \langle e_j | x_k \rangle$.

**We can further extend the set to an o.n. basis**

Let $\{|y_1\rangle, \ldots, |y_n\rangle\} \subseteq \mathbb{C}^n$ be a basis.

Find linearly independent columns of the matrix

$$[|e_1\rangle \cdots |e_m\rangle |y_1\rangle \cdots |y_n\rangle]$$

including the first $m$ columns.

Then apply Gram-Schmidt process.

**Example** Apply Gram-Schmidt to $\{|x_1\rangle, |x_2\rangle\}$ with

$$|x_1\rangle = \begin{pmatrix} 1 \\ 1 \\ i \end{pmatrix}, \; |x_2\rangle = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}.$$

Then extend the resulting set to an orthnormal basis.

**Basics of Matrices**

- Mixed quantum states are represented by density matrices, i.e., positive semi-definite matrices with trace 1.
- Observable / measurement operators correspond to Hermitian matrices.
- Quantum operations corresponds to unitary matrices.
- So, we need basic knowledge of matrices (relevant to quantum mechanics).

Let $\mathbf{M}_{m,n}$ be the set (vector space/algebra) of $m \times n$ complex matrices. If $m = n$, we let $\mathbf{M}_n = \mathbf{M}_{m,n}$.

- The set $\mathbf{M}_{m,n}$ is a vector space under addition and scalar multiplication.
- We can multiply $A = (a_{ij}) \in \mathbf{M}_{m,n}$ and $B = (b_{rs}) \in \mathbf{M}_{n,k}$ such that $C = AB = (c_{pq}) \in \mathbf{M}_{m,k}$ with

$$c_{pq} = (a_{p1}, \ldots, a_{pn}) \begin{pmatrix} b_{1q} \\ \vdots \\ b_{nq} \end{pmatrix} = \sum_{\ell=1}^{n} a_{p\ell} b_{\ell q}.$$

- If $A$ has rows $\langle A_1|, \ldots, \langle A_m|$ and $B$ has columns $|B_1\rangle, \cdots, |B_p\rangle$, then

$$AB = [A|B_1\rangle \cdots A|B_p\rangle] = \begin{pmatrix} \langle A_1|B \\ \vdots \\ \langle A_m|B \end{pmatrix}$$

**Block matrix multiplication.**

- If $A = (A_{ij}), B = (B_{rs})$ such that $A_{p\ell}B_{\ell q}$ is defined. That is, the number of columns of $A_{p\ell}$ equals the number of rows of $B_{\ell q}$.

- If $D = \operatorname{diag}(d_1, \ldots, d_n)$, $A$ has columns $|x_1\rangle, \ldots, |x_n\rangle$, and $B$ has rows $\langle y_1|, \ldots, \langle y_n|$, then

$$AD = [d_1|x_1\rangle \cdots d_n|x_n\rangle], \quad DB = \begin{pmatrix} d_1\langle y_1| \\ \vdots \\ d_n\langle y_n| \end{pmatrix},$$

$$AB = \sum_{j=1}^{n} |x_j\rangle\langle y_j|, \quad ADB = \sum_{j=1}^{n} d_j|x_j\rangle\langle y_j|.$$

- If $A \in \mathbf{M}_{m,n}, B \in \mathbf{M}_{n,k}, D = D_1 \oplus \mathbf{0}_{n-\ell}$, then

$$ADB = A_1D_1B_1,$$

  where $A_1$ is formed by the first $\ell$ columns of $A$ and $B_1$ is formed by the first $\ell$ rows of $B$.

**Eigenvalues**

- One can compute the eigenvalues and eigenvectors of $A \in \mathbf{M}_n$.
- This is done by solving the characteristic equation $\det(tI - A) = 0$, which is a polynomial equation.

  For every $t$ satisfying $\det(tI - A) = 0$, we solve for nonzero vectors $|x\rangle$ such that $A|x\rangle = t|x\rangle$.

**Special classes of matrices**

- $A \in \mathbf{M}_n$ is Hermitian if $A = A^\dagger$.

  The $(i, j)$ entry of $A$ is the conjugate of the $(j, i)$ entry of $A$.
- $A \in \mathbf{M}_n$ is unitary if $A^\dagger = A^{-1}$, i.e., $AA^\dagger = I_n$ or /and $A^\dagger A = I_n$.

  The columns of $U$ form an orthonormal basis for $\mathbb{C}^n$.
- $A \in \mathbf{M}_n$ is positive semidefinite if $\langle x|A|x\rangle \geq 0$ for all $|x\rangle \in \mathbb{C}^n$.

  Equivalently, $A$ is Hermitian with nonnegative eigenvalues.
- $A \in \mathbf{M}_n$ is normal if $AA^\dagger = A^\dagger A$.

**Normal matrices: Spectral decomposition & spectral theorem**

**Theorem** A matrix $A \in \mathbf{M}_n$ is normal if and only if there is a unitary $U = [|u_1\rangle \cdots |u_n\rangle]$ and unitary $D = \text{diag}\,(\lambda_1, \ldots, \lambda_n)$ such that

$$A = UDU^\dagger = \sum_{j=1}^{n} \lambda_j |u_j\rangle\langle u_j| \qquad (*).$$

That is $A$ has an orthonormal set of eigenvectors $\{|u_1\rangle, \ldots, |u_n\rangle\}$ for the eigenvalues $\lambda_1, \ldots, \lambda_n$ so that

$$A[|u_1\rangle \cdots |u_n\rangle] = [|u_1\rangle \cdots |u_n\rangle]D.$$

**Theorem** Suppose $A \in \mathbf{M}_n$ is normal in the form (*).

- If $k$ is a positive integer, then $A^k = \sum_{j=1}^n \lambda_j^k |u_j\rangle\langle u_j|$.
- If $A$ is invertible and $k$ is a positive integer, then $A^{-k} = \sum_{j=1}^n \lambda_j^{-k} |u_j\rangle\langle u_j|$.
- If $A$ has positive eigenvalues, then $A^r = \sum_{j=1}^n \lambda_j^r |u_j\rangle\langle u_j|$.
- If $f$ is an analytic function, then $f(A) = \sum_{j=1}^n f(\lambda_j) |u_j\rangle\langle u_j|$.

**Corollary** Let $A \in \mathbf{M}_n$.

- Then $A$ is Hermitian if and only if $A$ is normal with real eigenvalues.
- Then $A$ is unitary if and only if $A$ is normal with eigenvalues on of modulus 1.
- Then $A$ is positive semidefinite if and only if $A$ is normal (Hermitian) with nonnegative eigenvalues.

**Pauli matrices**:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

**Remark** If $A \in \mathbf{M}_2$ is Hermitian, then

$$A = (c_0, c_x, c_y, c_y) \cdot (\sigma_0, \sigma_x, \sigma_y, \sigma_z) = c_0 I_2 + c_x \sigma_x + c_y \sigma_z + c_z \sigma_z$$

with $c_0, c_x, c_y, c_z \in \mathbb{R}$.

**Example** In quantum computing, we often use $e^{iaA}$, where for a real unit vector $\mathbf{n} = (n_x, n_y, n_z)$ and $\sigma = (\sigma_x, \sigma_y, \sigma_z)$

$$A = \mathbf{n} \cdot \sigma = (n_x, n_y, n_z) \cdot (\sigma_x, \sigma_y, \sigma_z) = \begin{pmatrix} n_z & n_x - in_y \\ n_x + in_y & -n_z \end{pmatrix},$$

which has eigenvalues $1, -1$ and with eigenprojections

$$P_1 = \frac{1}{2}(I + A) = \begin{pmatrix} 1 + n_z & n_x - in_y \\ n_x + in_y & 1 - n_z \end{pmatrix}$$

and

$$P_2 = \frac{1}{2}(I - A) = \begin{pmatrix} 1 - n_z & -n_x + in_y \\ -n_x - in_y & 1 + n_z \end{pmatrix}.$$

Hence, $iaA = iaP_1 - iaP_2$ and

$$e^{iaA} = e^{ia} P_1 + e^{-ia} P_2 = \cos aI + i \sin aA.$$

**Singular value decomposition**

**Theorem** Let $A \in \mathbf{M}_{m,n}$. There are unitary $U \in \mathbf{M}_m$ and $V \in \mathbf{M}_n$ so that $U^\dagger AV = \Sigma$ such that the $(j, j)$ entries of $\Sigma$ is $s_j \geq 0$ for $1 \leq j \leq \min\{m, n\}$, where $s_1^2 \geq s_2^2 \geq \cdots$ are the eigenvalues of $A^\dagger A$.

Equivalently, there are positive numbers $s_1 \geq \cdots \geq s_k$ orthonormal sets $\{|u_1\rangle, \ldots, |u_k\rangle\} \subseteq \mathbb{C}^m$ and $\{|v_1\rangle, \ldots, |v_k\rangle\} \subseteq \mathbb{C}^n$ such that

$$A = \sum_{j=1}^{k} s_j |u_j\rangle\langle v_j|.$$

*Proof.* Suppose $V^\dagger A^\dagger AV = \mathrm{diag}\,(s_1^2, \ldots, s_n^2)$ with $s_1 \geq \cdots \geq s_n \geq 0$. Then the columns of $AV$ form an orthogonal set. Suppose the first $k$ columns of $AV$ are nonzero. Then $k \leq m$. Let $|u_i\rangle$ be the $i$th column of $AV$ divided by $s_i$, and let $U \in \mathbf{M}_m$ with the first $k$ columns equal to $|u_1\rangle, \ldots, |u_k\rangle$. Then $U^\dagger AV = \Sigma$. □

**Example** Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ i & i \end{pmatrix}$. Then $A^\dagger A = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$.

If $V = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, then $V^\dagger A A V = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$.

So, $\Sigma = \begin{pmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $AV = \begin{pmatrix} 2 & 0 \\ 0 & 0 \\ 2i & 0 \end{pmatrix}$.

We may take $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 \\ 0 & \sqrt{2} & 0 \\ i & 0 & -i \end{pmatrix}$ to get $U^\dagger A V = \Sigma$.

**Tensor products**

Let $A = (A_{ij})$ and $B$ be two rectangular matrices. Then their tensor product (Kronecker product) is the matrix

$$A \otimes B = (A_{ij} B).$$

This is very important. If $\rho_1, \rho_2$ are quantum states of two quantum systems, then $\rho_1 \otimes \rho_2$ is their product state in the bipartite (combined) system.

**Theorem** *For matrices $A, B, C, D$ of appropriate sizes, the following properties hold:*

(1) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

(2) $A \otimes (B + C) = A \otimes B + A \otimes C$,

(3) $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$,

(4) $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

*Proof.* (1) Let $A \in \mathbf{M}_{m,n}$, $B \in \mathbf{M}_{r,s}$, $C \in \mathbf{M}_{n,p}$, and $D \in \mathbf{M}_{s,q}$. If $AC = (\gamma_{rs})$, then

$$\begin{aligned}(A \otimes B)(C \otimes D) &= (a_{ij} B)(c_{ij} D) = (\gamma_{rs} BD) \\ &= (\gamma_{rs}) \otimes (BD) = (AC) \otimes (BD).\end{aligned}$$

(2) $A \otimes (B + C) = (A_{ij}(B + C))$

$$= (A_{ij} B) + (A_{ij} C) = A \otimes B + A \otimes C.$$

(3) Let $\gamma_{rs} = \bar{A}_{sr}$. Then

$$(A \otimes B)^\dagger = (A_{ij} B)^\dagger = (\gamma_{rs} B^\dagger) = A^\dagger \otimes B^\dagger.$$

(4) Note that $(A^{-1} \otimes B^{-1})(A \otimes B) = I \otimes I$. □

**Corollary** *For any matrices $A, B$, if*

$$R_1 A S_1 = T_1, R_2 B S_2 = T_2,$$

*then* $\quad (R_1 \otimes R_2)(A \otimes B)(S_1 \otimes S_2) = T_1 \otimes T_2.$

**Applications.**

- *Let $A \in \mathbf{M}_m, B \in \mathbf{M}_n$. If*

  $$S_1^{-1} A S_1 = D_1, S_2^{-1} B S_2 = D_2,$$

  *where $D_1, D_2$ are diagonal matrices, then*

  $$(S_1 \otimes S_2)^{-1}(A \otimes B)(S_1 \otimes S_2) = D_1 \otimes D_2$$

  *is a diagonal matrix.*

  ** If $A, B$ are normal, we may assume that $S_1, S_2$ be unitary.*

  ** If $A|u_i\rangle = \mu_i|u_i\rangle$ for $1 \leq i \leq m$, and $B|v_j\rangle = \nu_j|v_j\rangle$ $1 \leq j \leq n$, then*

  $$(A \otimes B)(|u_i v_j\rangle) = \mu_i \nu_j |u_i v_j\rangle,$$

  *where $|u_i v_j\rangle = |u_i\rangle \otimes |v_j\rangle$.*

- *If $A, B$ are rectangular matrices with singular decomposition*

  $A = \sum_{i=1}^{r} a_i |u_i\rangle\langle v_i|$ *and* $B = \sum_{j=1}^{s} b_j |x_j\rangle\langle y_j|$,

  *then*

  $$A \otimes B = \sum_{r,s} a_i b_j |u_i x_j\rangle\langle v_i y_j|$$

  *is the singular value decomposition of $A \otimes B$.*