Quantum Computation and Information

Swayam Chube

Last Compiled: June 2, 2022

Contents

Chapter 1

Introduction

Chapter 2

Quantum Mechanics

2.1 Linear Algebra Primer

I shall highlight only the notations and important results without spending far too long on rigorous proofs. The standard notation for a vector is $|\psi\rangle$ which is sometimes called a *ket*. We would mainly be interested in the study of *finite dimensional* vector spaces.

A *linear operator* between vector spaces V and W is defined to be any function $A : V \to W$ that is linear in its inputs, that it

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

The composition of the linear operators $A : V \to W$ and $B : W \to X$ is given by BA.

Now suppose $\{|v_i\rangle\}_{i=1}^m$ and $\{|w_i\rangle\}_{i=1}^n$ are basis for V and W respectively. Then, there exist complex numbers A_{ij} for each $1 \leq i \leq n$ and $1 \leq j \leq m$ such that

$$A|v_j\rangle = \sum_{i=1}^n A_{ij}|w_i\rangle$$

The *Pauli Matrices* are 2×2 complex matrices defined as:

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma_1 \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$
$$\sigma_2 \equiv Y \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

An *inner product* over a vector space V is simply a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ satisfying the following:

1. It is linear in its second argument. That is,

$$\left\langle |v_i\rangle, \sum_i \lambda_i |w_i\rangle \right\rangle = \sum_i \lambda_i \langle |v_i\rangle, |w_i\rangle\rangle$$

2. $\langle |v\rangle, |w\rangle\rangle = \langle |w\rangle, |v\rangle\rangle^*$
3. $\langle |v\rangle, |v\rangle\rangle \geq 0$ with equality if and only if $v = 0$.

A vector space equipped with an inner product is said to be an *inner product space*. Note that over finite dimensional comoplex vector spaces, a *Hilbert Space* is the same as an inner product space.

For an orthonormal basis of vectors $\{|i\rangle\}$, any arbitrary vector $|v\rangle$ may be written as $\sum_i v_i |i\rangle$ for some set of complex numbers v_i. Obviously, we have $\langle i|v\rangle = v_i$ and also,

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

This is known as the *completeness relation*. Then, for any linear operator $A : V \to W$, we may write:

$$\begin{aligned} A &= I_W A I_V \\ &= \sum_i \sum_j |w_j\rangle\langle w_j|A|v_i\rangle\langle v_i| \\ &= \sum_i \sum_j \langle w_j|A|v_i\rangle |w_j\rangle\langle v_i| \end{aligned}$$

which is its representation in *outer product form*. Here, $\{|v_i\rangle\}$ is the input basis while $\{|w_j\rangle\}$ is the output basis.

An *eigenvector* of a linear operator A on a vector space is a non-zero vector $|v\rangle$ such that $A|v\rangle = v|v\rangle$ where $v \in \mathbb{C}$ is known as the *eigenvalue* of A corresponding to $|v\rangle$. The *eigenspace* corresponding to an eigenvalue v is the set of eigenvectors of A having eigenvalue v.

A *diagonal representation* for A is a representation of the form

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

where the vectors $|i\rangle$ form an orthonormal set of eigenvectors for A with corresponding eigenvalues λ_i. These are also known as *orthonormal decompositions*. When an eigenspace is more than one-dimensional, we say that it is *degenerate*.

There exists a unique linear operator $A^\dagger$ such that for all $|v\rangle, |w\rangle \in V$,

$$\langle |v\rangle, A|w\rangle\rangle = \langle A^\dagger|v\rangle, |w\rangle\rangle$$

This linear operator is known as the *adjoint* or *Hermitian conjugate* of A. Obviously, that would mean, $(AB)^\dagger = B^\dagger A^\dagger$. By convension, if $|v\rangle$ is a vector, then we define $|v\rangle^\dagger = \langle v|$. Finally, we also note that $(A^\dagger)^\dagger = A$. An operator A whose adjoint is A is known as a *Hermitian* or *self-adjoint* operator.

Let V be an n-dimensional vector space and W be a k-dimensional vector subspace of V. Such that $|1\rangle, \ldots, |k\rangle$ is an orthonormal basis for W and $|1\rangle, \ldots, |n\rangle$ is an orthonormal subspace for V. Then, by definition,

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

is the *projector* onto the subspace W. It isn't hard to see that $P^\dagger = P$ and thus P is Hermitian, further, $P^2 = P$. The orthogonal complement of P is the operator $Q \equiv I - P$ which is a projector onto the vector space spanned by $|k+1\rangle, \ldots, |n\rangle$.

An operator A is said to be *normal* if $AA^\dagger = A^\dagger A$. It is obvious that a Hermitian operator is normal. A normal operator is Hermitian if and only if it has all real eigenvalues[1]

Theorem 2.1 (Spectral Decomposition). An operator M on a vector space V is *normal* if and only if it is *diagonal* with respect to some orthonormal basis for V.

An operator U is said to be *unitary* if $U^\dagger U = I$. All eigenvalues of a unitary matrix have modulus 1.

A special subclass of Hermitian operators is the *positive operators* which are such that for any vector $|v\rangle$, $\langle |v\rangle, A|v\rangle\rangle$ is a real, non-negative number. If $\langle |v\rangle, A|v\rangle\rangle$

[1] This follows trivially from the Spectral Decomposition Theorem

is strictly positive for all non-zero $|v\rangle$, then A is *positive definite*. One can show that every positive operator is necessarily Hermitian.

The *tensor product* is a way of putting vector spaces stogether to form larger vector spaces. This is useful in understanding the quantum mechanics of multi-particle systems. If V and W are vector spaces of dimension m and n respectively, then $V \otimes W$, read V *tensor* W, is an mn dimensional vector space. The elements of $V \otimes W$ are linear combinations of 'tensor products' $|v\rangle \otimes |w\rangle$ of elements $|v\rangle \in V$ and $|w\rangle \in W$. By definition, the tensor product satisfies the following properties:

1. For any scalar z,
$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$$
2. For $|v_1\rangle, |v_2\rangle \in V$,
$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$
3. For $|w_1\rangle, |w_2\rangle \in W$,
$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

Suppose A and B are linear operators on V and W respectively. Then we may define a linear operator $A \otimes B$ on $V \otimes W$ given by the equation

$$(A \otimes B)\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle\right) \equiv \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$$

It is easy to see that $A \otimes B$ is a well defined linear operator. We may also define an inner product on $V \otimes W$ as

$$\left\langle \sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle \right\rangle = \sum_i \sum_j \overline{a_i} b_j \langle v_i|v'_j\rangle \langle w_i|w'_j\rangle$$

Again, it is easy to see that the above is a well defined inner product. The abstract notion of a tensor product can be moved to a convenient matrix representation known as the *Kronecker product*. Suppose A is an $m \times n$ matrix and B is a $p \times q$ matrix, then we have

$$A \otimes B = \begin{bmatrix} A_{11}B & \dots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \dots & A_{mn}B \end{bmatrix}$$

which is an $mp \times nq$ matrix. Finally, we mention the useful notation $|\psi\rangle^{\otimes k}$ which means $|\psi\rangle$ tensored with itself k times.

A function $f : \mathbb{C} \to \mathbb{C}$ may be extended on normal matrices. We know that any normal operator has a spectral decomposition. Let

$$A = \sum_a a|a\rangle\langle a|$$

Then, define

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

This procedure may be used to define the square root of a positive operator, the logarithm of a positive definite operator or the exponential of a normal operator.

Another important matrix function is the *trace* of a matrix, which is defined to be the sum of its diagonal elements. The trace can be shown to be *cyclic*, that is $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. It then follows that the trace is invariant under the *unitary similarity transform*, $A \mapsto UAU^\dagger$ for a unitary matrix U. This ensures that the trace of an operator is well defined.

The *commutator* between two operators A and B is defined to be

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

while the *anti-commutator* is defined to be

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

If $[A, B] = 0$, then we say A *commutes* with B, similarly, if $\{A, B\} = 0$, then we say that A *anti-commutes* with B.

Theorem 2.2 (Simultaneous Diagonalization). Suppose A and B are Hermitian operators. Then $[A, B] = 0$ if and only if there exists an orthonormal basis such that both A and B are diagonal with respect to that basis. We say that A and B are *simultaneously diagonalizable* in this case.

Theorem 2.3 (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

$$A = UJ = KU$$

where the unique positive operators J and K satisfying these equations are defined by $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$.

We call $A = UJ$ the *left polar decomposition* of A and $A = KU$ the *right polar decomposition* of A. As a corollary of the above theorem, we have the *Singular Value Decomposition*.

Corollary 2.1. Let A be a square matrix. Then there exist unitary matrices U and V and a diagonal matrix D with non-negative entries such that

$$A = UDV$$

The diagonal elements of D are called the *singular values* of A.

2.2 Postulates of Quantum Mechanics

Postulate 1. Associated with any isolated physical system is a complex vector space with inner product (that is, Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector* which is a vector in the system's state space.

Postulate 2. The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle$$

The above postulate may be rephrased as follows:

Postulate 2′. The time evolution of the state of a closed quantum system is described by the *Schrödinger equation*

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where H is the Hamiltonian operator, which is Hermitian.

Because the Hamiltonian is Hermitian, it has a spectral decomposition:

$$H = \sum_E E|E\rangle\langle E|$$

The states $|E\rangle$ are conventionally referred to as *energy eigenstates* or sometimes as *stationary states*. The reason for this is because their only cahnge in time is:

$$|E\rangle \mapsto \exp(-iEt/\hbar)|E\rangle$$

One notes that this transformation does not change the fact that $|E\rangle$ are orthonormal. Let us now try to represent the unitary operator $U(t_1, t_2)$ in terms of H. Since the vectors $|E\rangle$ form an orthonormal basis for the Hilbert space, there exist constants c_E such that

$$|\psi(t_1)\rangle = \sum_E c_E|E\rangle$$

consequently, we may write:

$$|\psi(t_2)\rangle = \sum_E c_E \exp\left[-\frac{iE(t_2 - t_1)}{\hbar}\right]|E\rangle$$

As a result, we may write:

$$U(t_1, t_2) = \exp\left[-\frac{iH(t_2 - t_1)}{\hbar}\right]$$

It is easy to verify that U is indeed unitary. This establishes the equivalence between the two phrasings of **Postulate 2**.

Postulate 3. Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that the result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

The completeness relation then implies:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle$$

Further, we can show that *measurements cascade*. That is, if $\{L_l\}$ and $\{M_m\}$ are two sets of measurement operators, then a measurement defined by the measurement operators L followed by a measurement defined by the measurement operators M is physically equivalent to a single measurement defined by the measurement operators $\{N_{lm}\}$ with the representation $N_{lm} = M_m L_l$.

Distinguishing Quantum States

Projective Measurements

Definition 2.4 (Projective Measurement). A projective measurement is described by an *observable*, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues m of the observable. Upom measurement, the probability of getting m is given by

$$p(m) = \langle\psi|P_m|\psi\rangle$$

Given that the outcome m occurred, the state of the system immediately after the measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$$

Projective measurements are the most popular version of measurements described in most introductory books on Quantum Mechanics. This is because pro-

jective measurements have nice properties. For example:

$$\begin{aligned}\mathbb{E}[M] &= \sum_m m p(m) \\ &= \sum_m m \langle\psi|P_m|\psi\rangle \\ &= \langle\psi| \left(\sum_m m|P_m|\right) |\psi\rangle \\ &= \langle\psi|M|\psi\rangle\end{aligned}$$

POVM Measurements

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.

2.3 The Density Operator

Suppose a quantum system is in one of a number of states $|\psi_i\rangle$ with respective probabilities p_i. We hsall call $\{p_i, |\psi_i\rangle\}$ an *ensemble of pure states*. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

This operator is also known as the *density matrix*. If we allow this system to evolve, then there exists a unitary matrix U such that $|\psi_i\rangle \mapsto U|\psi_i\rangle$. And thus, $\rho \mapsto U\rho U^\dagger$.

Suppose now, we would like to perform a measurement described by measurement operators M_m. If the initial state was $|\psi_i\rangle$, then the probability of getting result m is

$$p(m \mid i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \text{tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|)$$

Then we may compute:

$$\begin{aligned} p(m) &= \sum_i p(m \mid i) p(i) \\ &= \sum_i p(i) \operatorname{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) \\ &= \operatorname{tr}(M_m^\dagger M_m \rho) \end{aligned}$$

If the initial state was $|\psi_i\rangle$, then the state after obtaining the result m is

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i}}$$

The density operator after obtaining a measurement of m is given by (after some simplifications)

$$\rho_m = \sum_i p(i \mid m) |\psi_i^m\rangle\langle\psi_i^m| = \frac{M_m \rho M_m^\dagger}{\operatorname{tr}(M_m^\dagger M_m \rho)}$$

A quantum system whose state is known exactly is said to be in a *pure state*. In this case, the density operator is $\rho = |\psi\rangle\langle\psi|$. Otherwise, ρ is in a mixed state. It can be shown that ρ corresponds to a pure state if and only if $\operatorname{tr}(\rho^2) = 1$. Else $\operatorname{tr}(\rho^2) < 1$ and it corresponds to a mixed state.

Theorem 2.5 (Characterization of Density Operators). An operator ρ is the density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if

1. (Trace Condition) ρ has trace equal to one
2. (Positivity Condition) ρ is a positive operator

We may now reformulate the postulates as follows

Postulate 1. Associated with any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *density operator*, which is a positive operator ρ with trace one, acting on the state space of the system. If a quantum system is in the state ρ_i with probability p_i, then the density operator of the system is $\sum_i p_i \rho_i$.

Postulate 2. The evolution of a closed quantum system is described by a *unitary transformation*. That is, ρ at a time t_1 is related to ρ' at a time t_2 by a unitary

operator U which depends only on times t_1 and t_2

$$\rho' = U\rho U^\dagger$$

Postulate 3. Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of teh system being measured. The index m refers to the measurement outcome. If the state of tue system is ρ immediately before the measurement, then the probability that the result m occurs is given by

$$p(m) = \text{tr}(M_m^\dagger M_m \rho)$$

and the state of the system after the measurement is

$$\frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I$$

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n and the system number i is prepared in the state ρ_i, then the joint state of the total system is $\rho_1 \otimes \cdots \otimes \rho_n$.

It is important to note that *different ensembles* can give rise to the same density matrix. For example, consider the density matrix

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$$

which is the density matrix corresponding to the ensemble

$$\left\{ \left(\frac{3}{4}, |0\rangle\right), \left(\frac{1}{4}, |1\rangle\right) \right\}$$

But, consider the following states:

$$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$$
$$|b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$$

Then, the same density operator corresponds to the ensemble

$$\left\{ \left(\frac{1}{2}, |a\rangle \right), \left(\frac{1}{2}, |b\rangle \right) \right\}$$