QCQI: Chapter 2 Summary

A Preprint

Krishna N Agaram

December 23, 2022

Abstract

1 A quick tour of Linear Algebra

2 The postulates of Quantum Mechanics

1. **(State space and vector)** *Associated with any isolated physical system is a Hilbert space called the state space of the system. The system is completely described by its state vector or wave function, which is a unit vector in the system's state space.*
   - Note that which state space and state vector are to be considered is not described by the postulate.
   - The state vector is often used in place of the system itself, for example, we may say 'this system is a unit vector in so-and-so state space'.
   - In Quantum Computation, we take the **qubit** as our fundamental quantum system. The qubit is a quantum system with a two-dimensional state space. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written $|\psi\rangle = a|0\rangle + b|1\rangle$ where $a, b \in \mathbb{C}$ satisfy $|a|^2 + |b|^2 = 1$. Indeed, there are real physical systems which may be described in terms of qubits. For now, though, it is sufficient to think of qubits in abstract terms, without reference to a specific realization.
2. **(Evolution in discrete time)** *The evolution of an isolated quantum system is described by a unitary transformation. That is, the state $|\psi'\rangle$ of the system at time t_2 is related to the state $|\psi\rangle$ of the system at time t_1 through a unitary transformation U which depends only on the times t_1 and t_2. That is,*

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

   Note that again, *which* U is to be taken is not described by the postulate. It turns out that for a single qubit, *any* unitary operator can be realized in realistic systems.

2' **(Evolution in continuous time)** *The time evolution of the state of a closed quantum system is described by the Schrodinger equation:*

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

which is a system of differential equations in dimension-of-state-space variables. H is a **hermitian** operator called the *Hamiltonian* of the system. Solving the equation we get the operator referenced in postulate 2 -

$$|\psi(t_2)\rangle = \exp\left(\frac{-i(t_2 - t_1)H}{\hbar}\right)|\psi(t_1)\rangle \implies U = U(t_1, t_2) = \exp\left(\frac{-i(t_2 - t_1)H}{\hbar}\right)$$

3. **(Measurement)** *Quantum measurements are described by a collection $\{M_m\}$ of measurement operators that satisfies **completeness**. These are operators acting on the state space of the system being measured. The*

index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

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

and the state of the system after the measurement is

$$|\psi_m'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^* M_m|\psi\rangle}}$$

Note that we must have (this is the completeness relation)

$$\sum_m M_m^* M_m = I$$

since $1 = \sum_m p(m) = \langle\psi| \left(\sum_m M_m^* M_m\right)|\psi\rangle$ for every state vector $|\psi\rangle$.

Remark. *Note that measurement is not a unitary operator applied to the system - well, it is not even deterministic! How is this a valid evolution of the state vector? The key to this apparent paradox is the fact that open systems (those which interact with the environment) need not obey unitary evolution, and indeed, if a system is being measured it must be interacting with the environment and so is open.*

This is a most general measurement operator definition. But usually, we work with what we call "measuring an observable". An <u>observable</u> is a hermitian operator M on the state space of the system being observed. Suppose it has the spectral decomposition $M = \sum_m mP_m$, with P_m being the projector onto the eigenspace with eigenvalue m. Then the measurement operators $\{M_m\}$ defined by $M_m = P_m$ for each m describe a so-called **projective measurement**. Clearly, this is a valid set of measurement operators, since

$$\sum_m P_m = \sum_i |i\rangle = I$$

where $|i\rangle$ is the orthonormal basis in the spectral decomposition for M. For a system in state vector $|\psi\rangle$, the *expectation* of an observable is defined to be

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

POVMs: Another type of measurement. Basically, if we don't really care about the state of the system after the measurement but rather only on the statistics of the measurement, then we might as well let $M_m^* M_m = E_m$ for each m and talk only of the E_m's - they are enough to compute the probabilities. Hence we get the following:

Definition (POVM Measurement)**.** *A POVM is a set of* ***positive*** *operators $\{E_m\}$ satisfying*

$$\sum_m E_m = I$$

Further, the probability of result m in the measurement is given by

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

Note that since for any such set $\{E_m\}$, the operators $\{\sqrt{E_m}\}$ form a valid set of measurement operators, so indeed a POVM can be easily turned into an actual set of measurement operators. The framework of POVMs is simpler than the general rule and very elegant. Note that under $E_m = P_m$, projective measurements are just a special case of a POVM.

Next, suppose we are interested in a composite system composed of multiple physical systems. Can we find the state vector of the composite system as a whole? The fourth postulate answers this question.

4. **[State vector of composite systems]** *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(-vector) of the total system is*

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

We will usually denote $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ by $|\psi_1\rangle|\psi_2\rangle \cdots |\psi_n\rangle$ or $|\psi_1\psi_2 \cdots \psi_n\rangle$.
Using this postulate, one can show that if unitary operations, projective measurements and the use of ancilla systems are allowed, any general measurement on a system can be realised. Hence, with unitary dynamics and ancilla systems, projective measurements are equivalent to general measurements.
Postulate 4 also enables us to define one of the most interesting and puzzling ideas associated with composite quantum systems - *entanglement*. We say that a state of a composite system that can't be written as a product of states of its component systems is an *entangled state*. This phenomenon is called entanglement, and it is often exploited in the design of quantum algorithms.

3 Superdense Coding

Alice wants to send Bob two (classical) bits. Can she do the job just by sending just one qubit to Bob? In other words, can we compress two bits into one qubit? Indeed, yes, if we allow Alice and Bob to share one each of a pair of pre-prepared qubits. We pre-prepare this pair in the bell statevector

$$|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

The two qubits are then divided. Suppose Alice got the first one. Then, based on the two bits $a, b \in 0, 1$ that Alice wants to send, she applies (on her qubit only) the operator $X^a Z^b$ (so on the pair, it is actually the operator $X^a Z^b \otimes I$ that's applied). The pair then takes one of the following four forms (where $|\psi_{ab}\rangle$ represents the final comined statevector if the message to be sent was ab). (These are called the **Bell basis/states**).

$$|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\psi_{01}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\psi_{10}\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$|\psi_{11}\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}}$$

They form an orthonormal basis of the pair's state space and so by a measurement they can be distinguished - which means, Bob can recover ab, as needed. To finish, we just

4 Density operators

The density operator language provides a convenient means for describing quantum systems whose state is not completely known. More precisely, suppose a quantum system is in one of a number of states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i. Each $|\psi_i\rangle$ is called a pure state. We shall call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. Note that the state of the system does not change between the $|\psi_i\rangle$'s of its own accord - it's just that we are not sure (we only have a distribution) which state it actually is in. The *density operator for the system* is defined by the equation

$$\rho := \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

The density operator is often known as the density matrix; we will use the two terms interchangeably. The key thing about the density operator is that it can be used *instead* of statevectors! Which is to say, instead of describing QM in terms of statevectors, we can describe it in terms of density operators instead. Plus, systems with ensembles instead of a well-known statevector are handled just as easily with this interpretation.

Suppose the system is closed and evolves in some duration according to unitary operator U. If it was in state $|\psi_i\rangle$, then this evolution takes it to $U|\psi_i\rangle$. So the new ensemble associated with the system after the evolution is $\{p_i, U|\psi_i\rangle\}$ with the density operator

$$\rho(t_2) = \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^* = U\rho(t_1)U^*$$

So postulate 2 can be rephrased without mention to any statevector, just in terms of the unitary matrix!

Similarly, we can rephrase measurement using

$$p(\text{we measure } m \mid \text{system is in } |\psi_i\rangle) = p(m|i) = \langle\psi_i|M_m^* M_m|\psi_i\rangle = \text{tr}(M_m^* M_m|\psi_i\rangle\langle\psi_i|),$$

giving

$$p(m) = \sum_i p(i)p(m|i) = \sum_i p_i\langle\psi_i|M_m^* M_m|\psi_i\rangle = \text{tr}(M_m^* M_m \rho).$$

If the result of the measurement is m, then the collapsed density operator is

$$\rho' = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^*}{\langle\psi_i|M_m^* M_m|\psi_i\rangle} = \sum_i p(m|i)\frac{p_i}{p(m)}\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^*}{p(m|i)} = \frac{M_m\rho M_m^*}{\text{tr}(M_m\rho M_m^*)}$$

Also note that for a composite system consisting of n systems, the i^{th} being an *independent* ensemble $\{p_j^{(i)}, |\psi_j^{(i)}\rangle\}_j$ (some of these could be pure, we can still represent them as an ensemble), then clearly the system is an ensemble of (by the multiplication of probabilities)

$$\{\prod_{i=1}^n p_{j_i}^{(i)}, \bigotimes_{i=1}^n |\psi_{j_i}^{(i)}\rangle\}_{j_1,\ldots,j_n}$$

giving the density operator

$$\begin{aligned}
\rho_{\text{composite}} &= \sum_{j_1,\ldots j_n}\left(\prod_{i=1}^n p_{j_i}^{(i)} \bigotimes_{i=1}^n |\psi_{j_i}^{(i)}\rangle\langle\psi_{j_i}^{(i)}|\right) \\
&= \sum_{j_1,\ldots j_n}\left(\bigotimes_{i=1}^n p_{j_i}^{(i)}|\psi_{j_i}^{(i)}\rangle\langle\psi_{j_i}^{(i)}|\right) \\
&= \bigotimes_{i=1}^n\left(\sum_{j_i} p_{j_i}^{(i)}|\psi_{j_i}^{(i)}\rangle\langle\psi_{j_i}^{(i)}|\right) \\
&= \rho_1 \otimes \ldots \otimes \rho_n
\end{aligned}$$

just like the relation for the statevectors!

Finally, all we have to do is characterize the density operator (like we did the statevector, the characterization it must be unit norm) to replace Postulate 1 and then QM is fully rephrased in density operator language, no statevector anywhere! The characterization is easy to see: any positive operator with trace 1 is a density operator for some ensemble and vice versa (the reverse is trivial, for the forward the ensemble with the p_i's being the eigenvalues and $|\psi_i\rangle$'s the eigenvectors gives us an ensemble), giving the rephrased postulate 1:

[Postulate 1, rephrased] *Associated to 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 for the system is $\sum_i p_i\rho_i$.*

The last line follows from expanding out each ρ_i in terms of its own ensemble, and then using basic probability to finish.

The Bloch sphere representation of a density operator

For a **qubit**, it can (easily) be shown that any density operator for the qubit is of the form

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}$$

where $\|\vec{r}\| \leq 1$. Equality holds iff the density operator represents a pure state. This vector $\vec{r}$ is called the Bloch sphere representation of the density operator. Hence each point inside and on the unit sphere represents a unique density operator for the qubit; points on the boundary represent the pure states. Sweet!

5 The reduced density operator

Suppose we know the density operator ρ^{AB} of a composite system AB. Could we then find/construct a density operator ρ_A for system A? We would like that we could use just this operator ρ_A for measurement (on A) statistics and it should all work out correctly. In other words, we want *a density operator ρ^A for system A on whose measurement we get the same measurement statistics as calculated from viewing the measurement as being done on the composite AB*. This is quite useful, and allows us to focus only on parts of the composite as we require.

More formally, suppose $\{E_m\}_m$ is a POVM for A. The POVM on AB corresponding to this POVM on A is, of course, $\{E_m \otimes I_B\}_m$. So the probability of outcome m is $\text{tr}((E_m \otimes I_B)\rho^{AB})$. Suppose we had a density operator ρ^A that indeed matched measurement statistics. That is, ρ^A must satisfy (for any set $\{E_m\}_m$) and any m the following:

$$\begin{aligned} \text{tr}(E_m \rho^A) &= p(m \text{ viewing measurement as done on } A) \\ &= p(m \text{ viewing measurement as done on } AB) \\ &= \text{tr}((E_m \otimes I_B)\rho^{AB}) \end{aligned}$$

We are looking for a function $f : \mathcal{L}(A \otimes B) \to \mathcal{L}(A)$ taking $\rho^{AB} \to \rho^A$. It can be shown that the above constraint for arbitrary positive E_m necessarily implies that $f \equiv \text{tr}_B$, where $\text{tr}_B : \mathcal{L}(A \otimes B) \to \mathcal{L}(A)$ is defined to be the linear operator satisfying

$$\text{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \otimes \langle b_2|b_1\rangle$$

for arbitrary $|a_1\rangle, |a_2\rangle \in A$, $|b_1\rangle, |b_2\rangle \in B$. Thus we get the ρ^A we needed:

$$\rho^A = \text{tr}_B\left(\rho^{AB}\right)$$

□