

Lecture 4: No Cloning, Entanglement, and Density Matrices

“[Entanglement is] not just one of many traits, but the characteristic trait of quantum physics. . .”
— Erwin Schrödinger

The primary focus of the next two lectures is to further practice working with quantum states and measurements, a natural avenue for which is the study of cloning, quantum entanglement, and non-local games. In the process, we will run into a more general formalism for describing quantum states, known as the *density operator* formalism. We begin in this lecture with cloning, quantum entanglement, and density operators.

1 No cloning theorem

One of the most natural operations we perform daily on classical computers is the act of copying or *cloning* classical bits. For example, you might make a copy of a file containing your LaTeX-typed homework to keep as a backup. On the negative side, a criminal might copy a classical object like a banknote (though it is not easy) to use as forged money. However, quantumly it turns out that copying quantum bits is impossible — given an arbitrary, unknown quantum state $|\psi\rangle \in \mathbb{C}^2$, there is no quantum circuit which creates a perfect copy of $|\psi\rangle$! How can we formalize such a statement?

We use proof by contradiction. Suppose there exists a unitary $U \in \mathcal{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ which, for *any* $|\psi\rangle$, maps $|\psi\rangle \otimes |0\rangle$ to $|\psi\rangle \otimes |\psi\rangle$, i.e. creates a copy of $|\psi\rangle$. To obtain the desired contradiction, we begin by applying U to two arbitrary states $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$, obtaining

$$|\phi\rangle = U(|\psi_1\rangle \otimes |0\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle \quad \text{and} \quad |\phi'\rangle = U(|\psi_2\rangle \otimes |0\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle.$$

What happens if we now take the inner product $\langle\phi|\phi'\rangle$? The middle terms of these equations yield

$$(\langle\psi_1| \otimes \langle 0|)U^\dagger U(|\psi_2\rangle \otimes |0\rangle) = (\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) = \langle\psi_1|\psi_2\rangle\langle 0|0\rangle = \langle\psi_1|\psi_2\rangle.$$

On the other hand, the right sides of the equations yield

$$(\langle\psi_1| \otimes \langle\psi_1|)(|\psi_1\rangle \otimes |\psi_1\rangle) = \langle\psi_1|\psi_2\rangle\langle\psi_1|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2.$$

Combining these two, we have that $\langle\psi_1|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2$ for some complex number $\langle\psi_1|\psi_2\rangle \in \mathbb{C}$. This is equivalent to saying $c = c^2$ for $c \in \mathbb{C}$, which has only two solutions — either $c = 1$ or $c = 0$. In other words, unless $|\psi_1\rangle$ and $|\psi_2\rangle$ are the same vector (in which case $\langle\psi_1|\psi_2\rangle = 1$) or are orthogonal (i.e. $\langle\psi_1|\psi_2\rangle = 0$), we have a contradiction. Thus, there does not exist a U which can perform the mapping $|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$ for arbitrary $|\psi\rangle$.

Exercise. This section showed that cloning arbitrary states $|\psi\rangle \in \mathbb{C}^2$ is impossible. However, the proof technique failed when the states $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal. Indeed, it turns out in this case cloning is possible. Give a quantum circuit which can clone states $|0\rangle$ and $|1\rangle$, i.e. maps $|0\rangle|0\rangle \mapsto |0\rangle|0\rangle$ and $|1\rangle|0\rangle \mapsto |1\rangle|1\rangle$. How about a circuit which clones $|+\rangle$ and $|-\rangle$? (Hint: Convert the $+/-$ basis into the standard basis first, then apply your cloning circuit for the standard basis.)

2 Quantum entanglement

We have already seen the concept of quantum entanglement, and in particular used Bell states such as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as a *resource* for performing interesting tasks such as quantum teleportation. But what exactly *is* entanglement, and how can we recognize whether a given state $|\psi\rangle$ is entangled?

History. First, a bit of history. The term “entanglement” was coined in 1935 by physicist Erwin Schrödinger, who used the term “Vershränkung”, which in colloquial “non-physicist” German means “folding of the arms”. As discussed in a previous lecture, the question of whether entanglement truly exists has been a subject of intense debate. The famous Einstein-Podolsky-Rosen paper of 1935, in particular, argued that quantum mechanics could not be a complete physical theory due to its prediction of entangled states such as $|\Phi^+\rangle$. In 1964, however, physicist John Bell proposed what is now known as a “Bell inequality” or “Bell test”; this test could in principle be run in a lab to confirm whether Nature indeed allows the strong type of correlations between qubits which entanglement would allow. Recently, such tests have been studied under the guise of “non-local games”, which is a topic we shall soon visit. Moreover, it is important to note that we nowadays know that any quantum computation (on pure quantum states) cannot achieve an exponential speedup over classical computers *unless* the amount of quantum entanglement in the system is “large”. Thus, entanglement is generally regarded as an important resource.

Bipartite entanglement. In this lecture, we study the notion of bipartite entanglement, meaning entanglement between a pair of quantum systems. Let $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ be an arbitrary bipartite state. How can we tell if $|\psi\rangle$ is entangled? Strictly speaking, earlier we defined $|\psi\rangle$ as *entangled* if it cannot be written as the tensor product of two states $|\psi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle \in \mathbb{C}^{d_2}$, i.e.

$$\forall |\psi_1\rangle \in \mathbb{C}^{d_1}, |\psi_2\rangle \in \mathbb{C}^{d_2} \quad \text{we have} \quad |\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi\rangle.$$

For example, let us confirm that $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled. Again, we give a proof by contradiction. Suppose there exist $|\psi_1\rangle \in \mathbb{C}^2, |\psi_2\rangle \in \mathbb{C}^2$ such that $|\psi_1\rangle \otimes |\psi_2\rangle = |\Phi^+\rangle$. If we write $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, we have

$$|\psi_1\rangle \otimes |\psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle.$$

Since this supposed to equal $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we must have $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$ (since the standard basis vectors $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are orthogonal). Suppose, without loss of generality, that $\beta_2 = 0$, so that $\alpha_1\beta_2 = 0$. Then, we must also have $\beta_1 = 0$ so that $\beta_1\alpha_2 = 0$ (the other option is to set $\alpha_2 = 0$, but this would yield $\alpha_2 = \beta_2 = 0$, i.e. $|\psi_2\rangle$ is not a unit vector). But if $\beta_1 = \beta_2 = 0$, then $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = |0\rangle$, so that $|\psi_1\rangle \otimes |\psi_2\rangle = |00\rangle \neq |\Phi^+\rangle$! Thus, we have a contradiction, and so $|\Phi^+\rangle$ is entangled.

The Schmidt decomposition. Rather than go through such proofs each time we wish to check if $|\psi\rangle$ is entangled, there is a more elegant tool we can use known as the *Schmidt decomposition*. To keep our discussion simple, we shall restrict our attention to the setting of two qubits; the ideas here extend straightforwardly to arbitrary local dimensions d_1 and d_2 . The Schmidt decomposition states that any vector $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ can be written in the following special form:

$$|\psi\rangle = \alpha_0|a_0\rangle|b_0\rangle + \alpha_1|a_1\rangle|b_1\rangle,$$

where the α_i are real and satisfy $\alpha_i \geq 0$, and where $\{|a_i\rangle\}_{i=0}^1$ and $\{|b_i\rangle\}_{i=0}^1$ are orthonormal bases for \mathbb{C}^2 . The number of non-zero α_i is called the *Schmidt rank* of $|\psi\rangle$.

Exercise. Verify that $|00\rangle$ and $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ are already written in terms of Schmidt decompositions. What are the Schmidt ranks of these two states?

Observe now that if $|\psi\rangle$ has Schmidt rank 1, then clearly it is not entangled, as its Schmidt decomposition is in tensor product form. And this is no coincidence — it turns out that an arbitrary state $|\psi\rangle$ is entangled if and only if its Schmidt rank is strictly greater than 1.

Exercise. Use the notion of Schmidt rank to answer the following: Is $|+\rangle|-\rangle$ entangled? How about $\sqrt{1/1000}|+\rangle|-\rangle + \sqrt{999/1000}|-\rangle|+\rangle$? Finally, how about $\frac{1}{\sqrt{2}}(|0\rangle|+\rangle - |0\rangle|-\rangle)$? (Hint: For this last one, be

careful! Is it written in its Schmidt decomposition?)

In this course, we shall not be tasked with *finding* Schmidt decompositions of states. However, like the spectral decomposition for matrices, when doing proofs it is often useful to know that bipartite states $|\psi\rangle$ can always be written in this way. Let us close by pointing out a subtle fact about Schmidt decompositions. Note that any vector $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ can be written as

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

This decomposition requires four terms (i.e. one per standard basis vector for \mathbb{C}^4). Part of the power of the Schmidt decomposition is that it manages to write this same state using just *two* terms.

3 Density matrices

We have delved further into the structure of entanglement and learned that a bipartite state $|\psi\rangle$ is entangled if and only if its Schmidt rank is at least 2. However, let's take a step back and return to our statement that $|\psi\rangle$ is entangled if it cannot be written as $|\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle \in \mathbb{C}^{d_2}$. Intuitively, states of the form $|\psi_1\rangle \otimes |\psi_2\rangle$, called *tensor product states*, are nice because one can immediately read off the state of each qubit — qubit one is in state $|\psi_1\rangle$, and qubit two in $|\psi_2\rangle$. Since entangled states cannot be written in tensor product form, however, this raises the question: How can we describe the state of qubit one in, say, the Bell pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$? The answer lies in a more general formalism for describing quantum states, known as the *density matrix formalism*.

Thus far, we have said that an arbitrary d -dimensional quantum state is described by a unit vector $|\psi\rangle$ in \mathbb{C}^d . Such states are called *pure* because we know exactly which state $|\psi\rangle$ we have. Now, suppose we play a game in which with probability $1/2$, I give you state $|\psi_1\rangle$, and with probability $1/2$, I give you state $|\psi_2\rangle$, and I don't tell you *which* state I've given you. How can you describe the quantum state in your possession, given that you don't know whether you actually have $|\psi_1\rangle$ or $|\psi_2\rangle$? This is done via the *density operator*

$$\rho = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2|. \quad (1)$$

More generally, if we play this game with m possible states $|\psi_i\rangle$, each given with probability p_i (i.e. $\sum_i p_i = 1$ and $p_i \geq 0$), then the density operator describing your system is

$$\rho = \sum_{i=1}^m p_i |\psi_i\rangle\langle\psi_i|.$$

Such a state is called *mixed* because you don't know with certainty which $|\psi_i\rangle$ you have in your possession. Let us make two important observations here.

1. *Mixtures vs. superpositions.* A mixture of states $\sum_i p_i |\psi_i\rangle\langle\psi_i|$ is entirely different than a superposition of states $\sum_i \alpha_i |\psi_i\rangle$. For starters, the former is a sum of matrices, whereas the latter is a sum of vectors. More importantly, the former models a state of ignorance about which $|\psi_i\rangle$ we actually have in our possession — we know our system is in *precisely one* such $|\psi_i\rangle$, but which one is unknown. In stark contrast, in a superposition, our system is in *all* of the states $|\psi_i\rangle$ simultaneously.
2. *Pure states.* If there is only one state $|\psi_i\rangle$ in the mixture, i.e. $p_i = 1$ for some i , then the mixture simply reads $\rho = |\psi_i\rangle\langle\psi_i|$. This state is called pure and has rank 1. Conversely, for any pure state $|\psi\rangle$, its density matrix is the rank 1 operator $\rho = |\psi\rangle\langle\psi|$.

Let us stress the first point above with a concrete example. The density matrix $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ is:

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{I}{2}.$$

In contrast, the state vector $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ is given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Note that former is a matrix, while the latter is a vector, i.e. these are completely different objects!

Exercise. What is the density matrix for pure state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$? Next, write down the 2×2 density matrix $\rho = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|+\rangle\langle +|$.

Let us now generalize our discussion further. A linear operator $\rho \in \mathcal{L}(\mathbb{C}^d)$ is called a *density matrix* if the following two properties hold:

- ρ is positive semi-definite, i.e. is Hermitian and has non-negative real eigenvalues, and
- ρ has trace 1, i.e. $\text{Tr}(\rho) = 1$.

Let us check that the density operators we have considered thus far satisfy these two properties. For example, for ρ from Equation (1), we have

$$\text{Tr}(\rho) = \text{Tr} \left(\frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2| \right) = \frac{1}{2}\text{Tr}(|\psi_1\rangle\langle\psi_1|) + \frac{1}{2}\text{Tr}(|\psi_2\rangle\langle\psi_2|) = \frac{1}{2}\langle\psi_1|\psi_1\rangle + \frac{1}{2}\langle\psi_2|\psi_2\rangle = 1.$$

As for the property of being positive semidefinite, we use the following fact: For any two positive semi-definite matrices A and B and real numbers $p, q \geq 0$, it holds that $pA + qB$ is also positive semi-definite. In particular, since both $|\psi_1\rangle\langle\psi_1|$ and $|\psi_2\rangle\langle\psi_2|$ are positive semi-definite (as you will show in the exercise below), we have that ρ is also positive semi-definite. Thus, ρ is a valid density operator.

Exercise. Why is $|\psi\rangle\langle\psi|$ positive semi-definite for *any* $|\psi\rangle$? (Hint: Use the spectral decomposition).

In fact, the requirements that $\text{Tr}(\rho) = 1$ and ρ be positive semidefinite allow us to recover exactly the interpretation of mixed states which this section started with — taking the spectral decomposition of ρ , we have

$$\rho = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|.$$

Since ρ is positive semidefinite, we know $\lambda_i \geq 0$ for all i . Moreover, recalling that $\text{Tr}(\rho) = \sum_i \lambda_i$, we know that since $\text{Tr}(\rho) = 1$, it holds that $\sum_i \lambda_i = 1$. Thus, $\{\lambda_i\}_i$ forms a probability distribution. This means that we can interpret ρ as follows: With probability λ_i , prepare state $|\lambda_i\rangle$. This is precisely the idea we started this section with! We thus have a good picture of how one can describe probabilistic mixtures over pure quantum states.

Exercise. Why are the Pauli gates X , Y , and Z not density matrices?

The maximally mixed state. Finally, let us consider a very special density matrix in $\mathcal{L}(\mathbb{C}^d)$, the *maximally mixed state* $\rho = I/d$ (where I denotes the identity matrix). Note that ρ is positive semidefinite since I is positive semidefinite (in fact, I has eigenvalues all equal to 1), and $\text{Tr}(I/d) = \frac{1}{d}\text{Tr}(I) = 1$. Thus, ρ is a valid density operator. But what exactly does I/d represent? Here, we use the fact that for any orthonormal basis $\{|\psi_i\rangle\}_{i=1}^d$ for \mathbb{C}^d , we have

$$\sum_{i=1}^d |\psi_i\rangle\langle\psi_i| = I.$$

In other words, for *any* orthonormal basis $\{|\psi_i\rangle\}_{i=1}^d$, ρ represents the following state: Pick state $|\psi_i\rangle$ with probability $1/d$, and prepare $|\psi_i\rangle$. Since this holds for any basis, we conclude that ρ gives us absolutely no information about which state $|\psi\rangle$ we actually have — *every* state is an eigenvector of ρ , and the eigenvalues of ρ form a uniform distribution. Thus, the maximally mixed state represents the case where we know *nothing* about the state of our system! This will be crucial when we discuss entanglement again below.

3.1 The partial trace operation

Our motivation in introducing density matrices stemmed from the fact that we did not know how to describe the state of qubit 1 in the Bell pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We claimed that the answer lies in the framework of density matrices, but we have not yet prescribed how one can *use* density matrices to describe the state of qubit 1 of $|\Phi^+\rangle$. We now do this via the *partial trace* operation.

Intuitively, given a bipartite density matrix ρ_{AB} on systems A and B , the partial trace operation $\text{Tr}_B(\rho_{AB})$ returns a density matrix on system A alone (analogously, $\text{Tr}_A(\rho_{AB})$ returns a density matrix on B alone). Formally, we have that

$$\text{Tr}_B : \mathcal{L}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}) \mapsto \mathcal{L}(\mathbb{C}^{d_1}).$$

How exactly is Tr_B defined? Recall that the trace of a matrix $\rho \in \mathcal{L}(\mathbb{C}^d)$ is defined as

$$\text{Tr}(\rho) = \sum_i \rho(i, i) = \sum_{i=1}^d \langle i | \rho | i \rangle.$$

For the *partial* trace, we copy this idea, except we only apply it to one subsystem as follows: For $\rho \in \mathcal{L}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$,

$$\text{Tr}_B(\rho) = \sum_{i=1}^{d_2} (I_A \otimes \langle i |) \rho (I_A \otimes | i \rangle).$$

In other words, we leave system A untouched (hence the I_A terms above), and “trace out” system B . Note that like the trace, the partial trace is a linear map. Let us practice this operation on a number of states, and in the process draw our desired connection to the Bell state which we started this lecture with.

Example 1: Product states. Suppose first that ρ is the density matrix of a pure product state $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. In other words,

$$\rho = (|\psi_1\rangle \otimes |\psi_2\rangle)(\langle\psi_1| \otimes \langle\psi_2|) = |\psi_1\rangle\langle\psi_1|_A \otimes |\psi_2\rangle\langle\psi_2|_B.$$

Recall that earlier we said the state of $|\psi\rangle$ on qubit 1 is exactly $|\psi_1\rangle$. Let us confirm this by applying the partial trace to ρ to trace out subsystem B :

$$\begin{aligned} \text{Tr}_B(\rho) &= \text{Tr}_B(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|) \\ &= \sum_{i=1}^d (I \otimes \langle i |) |\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2| (I \otimes | i \rangle) \\ &= \sum_{i=1}^d |\psi_1\rangle\langle\psi_1| \otimes \langle i | \psi_2 \rangle \langle \psi_2 | i \rangle \\ &= |\psi_1\rangle\langle\psi_1| \left(\sum_{i=1}^d \langle i | \psi_2 \rangle \langle \psi_2 | i \rangle \right) \\ &= |\psi_1\rangle\langle\psi_1| \text{Tr}(|\psi_2\rangle\langle\psi_2|) \\ &= |\psi_1\rangle\langle\psi_1|, \end{aligned}$$

where the second equality applies the definition of the partial trace, the second-last equality uses the definition of the trace, and the last equality uses the cyclic property of the trace. In other words, the state of qubit 1

is $|\psi_1\rangle$, as claimed! Note that the calculation above did not use the fact that $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ is pure — indeed, the same calculation yields that for any operator $\rho = \rho_1 \otimes \rho_2$,

$$\mathrm{Tr}_B(\rho) = \rho_1 \cdot \mathrm{Tr}(\rho_2). \quad (2)$$

Exercise. Show that for any $\rho = \rho_1 \otimes \rho_2$, $\mathrm{Tr}_A(\rho) = \mathrm{Tr}(\rho_1) \cdot \rho_2$. (Hint: Follow the chain of equalities in the calculation above.)

Example 2: Separable states. We have said that a pure state $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is not entangled, or *separable*, if and only if $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle \in \mathbb{C}^{d_2}$. This idea extends to the setting of mixed states as follows: A bipartite density matrix $\rho \in \mathcal{L}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ is unentangled or *separable* if

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|,$$

for some (possibly non-orthogonal) sets of vectors $\{|\psi_i\rangle\} \subseteq \mathbb{C}^{d_1}$ and $\{|\phi_i\rangle\} \subseteq \mathbb{C}^{d_2}$, and where the $\{p_i\}$ form a probability distribution. In other words, ρ is a probabilistic mixture of pure product states. An example of a separable state is

$$\rho = \frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|. \quad (3)$$

Since the partial trace is a linear map, and since we know that $\mathrm{Tr}_B(\rho_1 \otimes \rho_2) = \rho_1 \cdot \mathrm{Tr}(\rho_2) = \rho_1$ for density matrices ρ_1, ρ_2 , computing the partial trace of ρ for separable states is simple:

$$\mathrm{Tr}_B\left(\sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|\right) = \sum_i p_i \mathrm{Tr}_B(|\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|) = \sum_i p_i |\psi_i\rangle\langle\psi_i| \cdot \mathrm{Tr}(|\phi_i\rangle\langle\phi_i|) = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Exercise. What is $\mathrm{Tr}_B(\rho)$ for ρ from Equation (3)?

Let us make one further comment about mixed separable states. We saw earlier that it is “easy” to check if a bipartite pure state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is entangled by determining its Schmidt rank (we did not explicitly state this, but the Schmidt rank can be calculated in time polynomial in the dimension d). In stark contrast, it turns out that determining whether a *mixed* state $\rho \in \mathcal{L}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is separable is NP-hard! This is another strong reminder that the settings of pure versus mixed states are indeed very different; the latter is typically much more difficult to work with.

Example 3: Pure entangled states. We finally arrive at the case we started this lecture with: Pure entangled states such as $|\Phi^+\rangle$. To compute the partial trace of any pure bipartite $|\psi\rangle$, one approach is to simply write out $|\psi\rangle$ in the standard basis, take its density matrix $\rho = |\psi\rangle\langle\psi|$, and then compute $\mathrm{Tr}_B(\rho)$. For example, for $|\Phi^+\rangle$, we have

$$\begin{aligned} \mathrm{Tr}_B(|\Phi^+\rangle\langle\Phi^+|) &= \frac{1}{2}\mathrm{Tr}_B((|00\rangle + |11\rangle)(\langle 00| + \langle 11|)) \\ &= \frac{1}{2}\mathrm{Tr}_B(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \\ &= \frac{1}{2}\mathrm{Tr}_B(|00\rangle\langle 00|) + \frac{1}{2}\mathrm{Tr}_B(|00\rangle\langle 11|) + \frac{1}{2}\mathrm{Tr}_B(|11\rangle\langle 00|) + \frac{1}{2}\mathrm{Tr}_B(|11\rangle\langle 11|) \\ &= \frac{1}{2}\mathrm{Tr}_B(|0\rangle\langle 0| \otimes |0\rangle\langle 0|) + \frac{1}{2}\mathrm{Tr}_B(|0\rangle\langle 1| \otimes |0\rangle\langle 1|) + \frac{1}{2}\mathrm{Tr}_B(|1\rangle\langle 0| \otimes |1\rangle\langle 0|) + \frac{1}{2}\mathrm{Tr}_B(|1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\ &= \frac{1}{2}|0\rangle\langle 0|\mathrm{Tr}(|0\rangle\langle 0|) + \frac{1}{2}|0\rangle\langle 1|\mathrm{Tr}(|0\rangle\langle 1|) + \frac{1}{2}|1\rangle\langle 0|\mathrm{Tr}(|1\rangle\langle 0|) + \frac{1}{2}|1\rangle\langle 1|\mathrm{Tr}(|1\rangle\langle 1|) \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\ &= \frac{1}{2}I, \end{aligned}$$

where the third equality follows from the linearity of the partial trace, the fifth by Equation (2), and the sixth by the cyclic property of the trace and since $|0\rangle$ and $|1\rangle$ are orthogonal. Thus, the reduced state on qubit 1 for the Bell state is *maximally mixed*! In other words, it is a completely random state about which we have *zero* information. In a similar fashion, one can show that $\text{Tr}_A(|\Phi^+\rangle\langle\Phi^+|) = I/2$.

Exercise. Show that $\text{Tr}_A(|\Phi^+\rangle\langle\Phi^+|) = I/2$.

And here we arrive at one of the most confounding aspects of quantum mechanics: As in the case of the Bell state, it is possible for us to know *absolutely nothing* about the states of qubits 1 and 2 individually (e.g. they have reduced states $I/2$), but when we bring both qubits together, we know *everything* about their joint state (e.g. $|\Phi^+\rangle$ is a pure state, i.e. there is no uncertainty). This is yet another striking example of a quantum phenomenon which does not occur in the classical world.

3.2 Using partial trace to detect entanglement

Recall that in Section 2, we said that an arbitrary bipartite *pure* state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ can be written in terms of its Schmidt decomposition

$$|\psi\rangle = \sum_i \alpha_i |a_i\rangle |b_i\rangle,$$

where $\alpha_i \geq 0$ and $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$ are orthonormal sets. We also said that $|\psi\rangle$ is entangled if and only if its Schmidt rank (i.e. number of non-zero Schmidt coefficients α_i) is at least two. However, we did not discuss how to actually *find* the Schmidt decomposition of $|\psi\rangle$, i.e. we have not specified a procedure for computing the Schmidt rank of $|\psi\rangle$. The partial trace allows us to solve this problem.

Exercise. Prove that the Schmidt rank of $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ equals the rank of $\rho_A = \text{Tr}_B(|\psi\rangle\langle\psi|)$. You should use the fact that in the definition of the partial trace, the standard basis $\{|i\rangle\}$ on B can be replaced by an arbitrary orthonormal basis, $\{|\psi_i\rangle\}$, on B . (Hint: Choose $\{|\psi_i\rangle\}$ as the Schmidt basis for $|\psi\rangle$ on system B .)

The exercise above immediately gives us a method for determining whether a bipartite pure state $|\psi\rangle$ is entangled — namely, compute $\rho_A = \text{Tr}_B(|\psi\rangle\langle\psi|)$, and check if $\text{rank}(\rho_A) > 1$. If so, $|\psi\rangle$ is entangled; otherwise, it is a product state. Finally, observe that this trick only works for *pure* states $|\psi\rangle$ — indeed, for mixed bipartite ρ_{AB} , detecting entanglement is NP-hard, so such a simple criterion for entanglement is highly unlikely to exist!

3.3 How the postulates of quantum mechanics apply to density operators

In previous lectures, we introduced the postulates of quantum mechanics in the context of pure states $|\psi\rangle$. All four postulates extend naturally to the setting of mixed quantum states. For example, for Postulate 3 on composite quantum systems, given density operators ρ and σ , we have that $\rho \otimes \sigma$ is also a valid density operator. This follows from the facts that if A and B are positive semi-definite, then so is $A \otimes B$, and that $\text{Tr}(A \otimes B) = \text{Tr}(A)\text{Tr}(B)$. For now, we will avoid revisiting the postulates in the mixed state setting, and rather approach the topic once the need arises in specific applications of future lectures.