Notes 8.370/18.435 Fall 2022

Lecture 5 Prof. Peter Shor

In the previous few lectures, we saw how to operate on one qubit—or more generally, one d-dimensional quantum system. We studied how to transform quantum systems with a unitary matrix, and how to measure them via a complete set of projection matrices. In this lecture, we explain how the state space of a joint quantum system, composed of two individual quantum systems, is constructed.

Suppose we have two quantum systems. Each of these has a state space which is a complex vector space of dimensions d_1 and d_2, respectively. When we consider these two quantum systems together, we get a state space which is the tensor product of their individual state spaces, and which has dimension $d_1 d_2$.

Some of you probably haven't see tensor products before. We will show how it works by exammple. If you have two qubits, each of which has a state space with basis $\{|\,0\rangle, |\,1\rangle\}$, then the state space of the joint system has basis

$$\{|\,0\rangle \otimes |\,0\rangle, |\,0\rangle \otimes |\,1\rangle, |\,1\rangle \otimes |\,0\rangle, |\,1\rangle \otimes |\,1\rangle\}.$$

The convention is to write the basis in lexicographical order. Thus, if you have two qubits in state $\alpha_0 |\,0\rangle + \alpha_1 |\,1\rangle$ and $\beta_0 |\,0\rangle + \beta_1 |\,1\rangle$, the system of both qubits is in state

$$\alpha_0\beta_0 |\,0\rangle \otimes |\,0\rangle + \alpha_0\beta_1 |\,0\rangle \otimes |\,1\rangle + \alpha_1\beta_0 |\,1\rangle \otimes |\,0\rangle + \alpha_1\beta_1 |\,1\rangle \otimes |\,1\rangle,$$

so the standard distributed law applies to tensor products. Often, rather than writing $|\,0\rangle \otimes |\,1\rangle$, we will write this as $|\,01\rangle$.

To illustrate tensor products using a more usual vector notation,

$$\begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

What if you have n qubits? The state space has dimension 2^n, and has basis $|\,00\ldots00\rangle$, $|\,00\ldots01\rangle$, $|\,00\ldots10\rangle$, …. (Recall that by notation, $|\,00\ldots00\rangle = |\,0\rangle \otimes |\,0\rangle \otimes \ldots \otimes |\,0\rangle \otimes |\,0\rangle$.)

Now let us count up (real) degrees of freedom. A qubit has a state $\alpha |\,0\rangle + \beta |\,1\rangle$, and since α and β are complex numbers, this would give four real degrees of freedom. However, it also satisfies $i|\alpha|^2 + |\beta|^2 = 1$, which means that it only has three real degrees of freedom (if we use the fact that multiplying by a global phase leaves the state essentially unchanged, there are only two degrees of freedom). However, the joint state of two qubits has four complex coefficients, leaving 7 (or 6) degrees of freedom. Thus, because $7 > 2 \cdot 3$, there are some states of the joint system which cannot be the tensor product of states of the individual systems. These states are called *entangled*. In fact, because the number of degrees of freedom of tensor product states is less than that of entangled states, the tensor product states form a lower-dimensional manifold in the entangled states, and we see that most quantum states are entangled.

For example, the state

$$\frac{1}{\sqrt{3}}\,|\,00\rangle+\frac{1}{\sqrt{3}}\,|\,01\rangle+\frac{1}{\sqrt{6}}\,|\,10\rangle+\frac{1}{\sqrt{6}}\,|\,11\rangle = \left(\frac{\sqrt{2}}{\sqrt{3}}\,|\,0\rangle + \frac{1}{\sqrt{3}}\,|\,1\rangle\right)\left(\frac{1}{\sqrt{2}}\,|\,0\rangle + \frac{1}{\sqrt{2}}\,|\,1\rangle\right)$$

is a tensor product state, while the state

$$\frac{1}{\sqrt{3}}\,|\,00\rangle + \frac{1}{\sqrt{3}}\,|\,01\rangle + \frac{1}{\sqrt{3}}\,|\,10\rangle$$

is entangled You can see that the second one is not a tensor product state, and thus entangled, because if we could represent it as a tensor product state

$$\alpha_0\beta_0\,|\,00\rangle + \alpha_0\beta_1\,|\,01\rangle + \alpha_1\beta_0\,|\,10\rangle + \alpha_1\beta_1\,|\,11\rangle\,,$$

then we would need $\alpha_1\beta_1 = 0$. But if that holds, either α_1 or β_1 is 0, so one of $\alpha_0\beta_1$ and $\alpha_1\beta_0$ must be 0, which is not the case.

What about unitary transformations on a joint state space. Suppose we have two unitary matrices U and V, of dimensions k and ℓ. The tensor product of them is the $k\ell \times k\ell$ matrix

$$U \otimes V = \begin{pmatrix} u_{11}V & u_{12}V & \dots & u_{1k}V \\ u_{21}V & u_{22}V & \dots & u_{2k}V \\ \vdots & \vdots & & \vdots \\ u_{k1}V & u_{k2}V & \dots & u_{kk}V \end{pmatrix},$$

where $u_{ij}V$ is the (i, j) entry of U multiplied by V.

Let's do an example and figure out what $\sigma_x \otimes \sigma_z$ is. We have

$$\begin{aligned} \sigma_x \otimes \sigma_z &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{array}\right) \end{aligned}$$

If the input is in a tensor product state $|\,\phi_1\rangle \otimes |\,\phi_2\rangle$, and you apply a tensor product unitary $U_1 \otimes U_2$, then the output is also in a tensor product state, namely $U_1\,|\,\phi_1\rangle \otimes U_2\,|\,\phi_2\rangle$. So to get an entangled output from a tensor product input, you need to apply a unitary that is not a tensor product. One non-tensor-product unitary that we will be using extensively in this class is the CNOT.

We have

$$\begin{aligned} CNOT &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= |\,0\rangle\langle 0\,| \otimes I + |\,1\rangle\langle 1\,| \otimes \sigma_x \end{aligned}$$

The last description says that if the first qubit is a $|\,0\rangle$, then we apply an identity to the second qubit, and if the first qubit is a $|\,1\rangle$, we apply a σ_x (or NOT gate) to the second qubit. This is why it's called a controlled NOT — depending on the state of the first qubit, we apply a NOT gate to the second one (or we don't).

Note that we don't measure the first qubit — we don't get a classical record of the state of the first qubit, and a state that was in a superposition of the first qubit being $|\,0\rangle$ and$|\,1\rangle$ remains in a superposition. Let's do an example. Suppose we start with the state $|\,+\rangle\,|\,0\rangle = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,10\rangle)$. When we apply the CNOT gate, the $|\,00\rangle$ remains unchanged, because the first qubit is $|\,0\rangle$, but the $|\,10\rangle$ becomes $|\,11\rangle$. This means

$$\mathrm{CNOT}\,|\,+\rangle\,|\,0\rangle = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle),$$

so we have used the CNOT gate to entangle two qubits.