CS 294-2 Hilbert Spaces, Super-dense coding, Teleportation 1/24/07
Spring 2007 Lecture 3

0.1 Tensor Products

Consider two quantum systems - the first with k distinguishable (classical) states (associated Hilbert space $\mathscr{C}^k$), and the second with l distinguishable states (associated Hilbert space $\mathscr{C}^l$). What is the Hilbert space associated with the composite system? We can answer this question as follows: the number of distinguishable states of the composite system is kl — since for each distinct choice of basis (classical) state $|i\rangle$ of the first system and basis state $|j\rangle$ of the second system, we have a distinguishable state of the composite system. Thus the Hilbert space associated with the composite system is $\mathscr{C}^{kl}$.

The tensor product is a general construction that shows how to go from two vector spaces V and W of dimension k and l to a vector space $V \otimes W$ (pronounced "V tensor W") of dimension kl. Fix bases $|v_1\rangle, \ldots, |v_k\rangle$ and $|w_1\rangle, \ldots, |w_l\rangle$ for V, W respectively. Then a basis for $V \otimes W$ is given by

$$\{|v_i\rangle \otimes |w_j\rangle : 1 \leq i \leq k, 1 \leq j \leq l\},$$

so that $\dim(V \otimes W) = kl$. So a typical element of $V \otimes W$ will be of the form $\sum_{ij} \alpha_{ij}(|v_i\rangle \otimes |w_j\rangle)$. We can define an inner product on $V \otimes W$ by

$$(|v_1\rangle \otimes |w_1\rangle, |v_2\rangle \otimes |w_2\rangle) = (|v_1\rangle, |v_2\rangle) \cdot (|w_1\rangle, |w_2\rangle),$$

which extends uniquely to the whole space $V \otimes W$.

For example, consider $V = \mathscr{C}^2 \otimes \mathscr{C}^2$. V is a Hilbert space of dimension 4, so $V \cong \mathscr{C}^4$. So we can write $|00\rangle$ alternatively as $|0\rangle \otimes |0\rangle$. More generally, for n qubits we have $\mathscr{C}^2 \otimes \cdots$ (n times) $\otimes \cdots \mathscr{C}^2 \cong \mathscr{C}^{2^n}$. A typical element of this space is of the form

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle.$$

0.2 Measurements

Let $|\phi\rangle \in \mathscr{C}^k$ be the quantum state of a k-state system. Then a measurement of $|\phi\rangle$ is a process that specifies an orthonormal basis $\{|v_j\rangle\}$ for $\mathscr{C}^k$, and associates a real number r_j with each basis vector. In the case that the r_j's are distinct, the outcome of the measurement is r_j with probability $|\langle v_j| |\phi\rangle|^2$, and in that case the new state is $|v_j\rangle$. If the r_j's are not distinct, then consider the subspace spanned by all $ketv_j$'s with associated real number $r_j = r$, and let P be the projection operator that projects into this subspace. Then the measurement outcome is r with probability $|P|\phi\rangle|^2$, and in that case the new state is $\frac{P|\phi\rangle}{|P|\phi\rangle|}$.

Another way of describing an orthogonal measurement is by a Hermitian operator M. Such an operator has an orthogonal set of eigenspaces, each with a real eigenvalue. These provide the measurement basis together with the associated real numbers. The Hermitian operator corresponding to the above orthogonal measurement is just $\sum_j r_j |v_j\rangle \langle v_j|$.

0.3 Quantum Gates

Recall the examples of simple unitary transforms, or "quantum gates." These include the single qubit gates such as the hadamard gate H, the NOT gate X, the controlled phase gate Z, the rotation by θ gate R_θ, as well as the two qubit gate $CNOT$.

Certain families of quantum gates are universal in the sense that any unitary transformation on k qubits can be closely approximated by a quantum circuit using only quantum gates from the family. Of course, the number of quantum gates in the circuit must scale exponentially in k. Examples of universal families of quantum gates include CNOT and all single qubit gates (actually any single qubit gate other than the Hadamard).

0.4 Tensor product of operators

Suppose we have two quantum systems: a k-state system with associated Hilbert space V and a l-state system with associated Hilbert space W. Suppose we apply a unitary transformation A to the first system and B to the second system. What is the resulting transformation on the combined system $V \otimes W$? To figure this out, let us first see how the combined transformation acts on basis states of $V \otimes W$. Consider a basis state $|i\rangle \otimes \{ket\, j$ where $0 \le i \le k-1$ and $0 \le j \le l-1$. Since A is only acting on V and B only on W, this state is transformed to $A|i\rangle \otimes B|j\rangle$.

Suppose $|v\rangle$ and $|w\rangle$ are unentangled states on $\mathscr{C}^m$ and $\mathscr{C}^n$, respectively. The state of the combined system is $|v\rangle \otimes |w\rangle$ on $\mathscr{C}^{mn}$. If the unitary operator A is applied to the first subsystem, and B to the second subsystem, the combined state becomes $A|v\rangle \otimes B|w\rangle$.

In general, the two subsystems will be entangled with each other, so the combined state is not a tensor-product state. We can still apply A to the first subsystem and B to the second subsystem. This gives the operator $A \otimes B$ on the combined system, defined on entangled states by linearly extending its action on unentangled states.

(For example, $(A \otimes B)(|0\rangle \otimes |0\rangle) = A|0\rangle \otimes B|0\rangle$. $(A \otimes B)(|1\rangle \otimes |1\rangle) = A|1\rangle \otimes B|1\rangle$. Therefore, we define $(A \otimes B)(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle)$ to be $\frac{1}{\sqrt{2}}(A \otimes B)|00\rangle + \frac{1}{\sqrt{2}}(A \otimes B)|11\rangle = \frac{1}{\sqrt{2}}\left(A|0\rangle \otimes B|0\rangle + A|1\rangle \otimes B|1\rangle\right)$.)

Let $|e_1\rangle, \ldots, |e_m\rangle$ be a basis for the first subsystem, and write $A = \sum_{i,j=1}^m a_{ij}|e_i\rangle\langle e_j|$ (the i,jth element of A is a_{ij}). Let $|f_1\rangle, \ldots, |f_n\rangle$ be a basis for the second subsystem, and write $B = \sum_{k,l=1}^n b_{kl}|f_k\rangle\langle f_l|$. Then a basis for the combined system is $|e_i\rangle \otimes |f_j\rangle$, for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. The operator $A \otimes B$ is

$$\begin{aligned}
A \otimes B &= \left(\sum_{ij} a_{ij}|e_i\rangle\langle e_j|\right) \otimes \left(\sum_{kl} b_{kl}|f_k\rangle\langle f_l|\right) \\
&= \sum_{ijkl} a_{ij}b_{kl}|e_i\rangle\langle e_j| \otimes |f_k\rangle\langle f_l| \\
&= \sum_{ijkl} a_{ij}b_{kl}(|e_i\rangle \otimes |f_k\rangle)(\langle e_j| \otimes \langle f_l|) \ .
\end{aligned}$$

Therefore the $(i,k),(j,l)$th element of $A \otimes B$ is $a_{ij}b_{kl}$. If we order the basis $|e_i\rangle \otimes |f_j\rangle$ lexicographically, then the matrix for $A \otimes B$ is

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} ;$$

in the i, jth subblock, we multiply a_{ij} by the matrix for B.

0.5 Bell States

The following simple quantum circuit on two qubits outputs one of the four Bell basis states as the inputs range over the two bit strings.

FIGURE of quantum circuit with Hadamard gate followed by CNOT.

The four Bell basis states are denoted:

$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)$

$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)$

$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)$

$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle)$

The state Ψ^-, also called the singlet state, has the special property that it is invariant under a unitary change of basis of the two qubits (same change of basis for both qubits).

1 Superdense Coding

Suppose Alice and Bob have a *quantum* communications channel, over which Alice can send qubits to Bob. However, Alice just wants to send a regular classical letter (sequence of bits). One way to send her message is to encode a 0 as $\left|0\right\rangle$ and a 1 as $\left|1\right\rangle$. But can she do better than sending as many qubits as bits in her message?

Intuitively, since quantum systems are more complex than classical systems, they can hold information – so maybe Alice can do better. But quantum information is hard to access; when you measure a quantum state, it looks classical – so maybe she can't.

In fact, if Alice and Bob share a Bell state, then she can send two classical bits of information using only one qubit.

Say Alice and Bob share $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)$. Depending on the message Alice wants to send, she applies a gate to her qubit, then sends it to Bob. If Alice wants to send 00, then she does nothing to her qubit, just sends it to Bob. If Alice wants to send 01, she applies the phase flip Z to her qubit, changing the quantum state to $\frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle) = \left|\Phi^-\right\rangle$. To send 10, she applies the NOT gate, giving $\frac{1}{\sqrt{2}}(\left|10\right\rangle + \left|01\right\rangle) = \left|\Psi^+\right\rangle$. To send 11, she applies both NOT and Z, giving $\frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle) = \left|\Psi^-\right\rangle$.

After receiving the qubit from Alice, Bob has one of the four mutually orthogonal Bell states. He can therefore apply a measurement to distinguish between them with certainty, and determine Alice's message. In practice, the way he'll make this measurement is by running the circuit we saw in Lecture 2 backwards (i.e., applying $(H \otimes I) \circ CNOT$), then measuring in the standard basis.

Note that Alice really did use two qubits total to send the two classical bits. After all, Alice and Bob somehow had to start with a shared Bell state. However, the first qubit – Bob's half of the Bell state – could have been sent well before Alice had decided what message she wanted to send. Perhaps only much later did she decide on her message and send over the second qubit.

One can show that it is not possible to do any better. Two qubits are necessary to send two classical bits. Superdense coding allows half the qubits to be sent before the message has been chosen.

1.1 Another Example: Quantum Teleportation

The *No Cloning Theorem* states that no quantum system can copy a qubit; that is, there is no transform sending $|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$. However, if we are willing to destroy the original, we can transmit a qubit, even to a remote location.

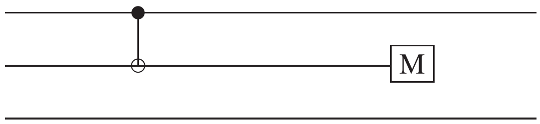
Suppose A has access to a quantum state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, which she wants to transmit to a remote party B. She can accomplish this by transmitting only classical bits of information, provided A and B share the entangled two-qubit state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The technique is known as *quantum teleportation.*

The basic idea is this. A controls $|\psi\rangle$ and the first qubit of $|\phi\rangle$. A's strategy, roughly speaking, is to forcibly entangle $|\psi\rangle$ with the first qubit $|\phi\rangle$. A then measures the first qubit of $|\phi\rangle$, resolving it completely, and hopes this will cause $|\psi\rangle$ to become entangled with the *second* qubit of $|\phi\rangle$. Presumably, B could then transfer $|\psi\rangle$ to the second qubit of $|\phi\rangle$.

As a first try, consider the following diagram. The top line represents $|\psi\rangle$; the bottom two represent the two qubits of $|\phi\rangle$.



That is, A passes $|\psi\rangle$ and the first qubit of $|\phi\rangle$ through a CNOT gate, and then measures the first qubit of $|\phi\rangle$. Now the input into the system as a whole is

$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=0,1} a_i|i\rangle \otimes \sum_{j=0,1} \frac{1}{\sqrt{2}}|j,j\rangle.$$

After passing through the CNOT gate this becomes

$$\sum_{i,j} a_i \big| i, i \oplus j, j \big\rangle.$$

Now A measures the middle qubit. Suppose it is measured as l; then $l = i \oplus j$. The state is now

$$\sum_j a_{j\oplus l} \big| j \oplus l, j \big\rangle.$$

Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip on his qubit (the bottom qubit in the diagram.) A bit flip is just the transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we have

$$\sum_j a_{j\oplus l} \big| j, j \big\rangle.$$

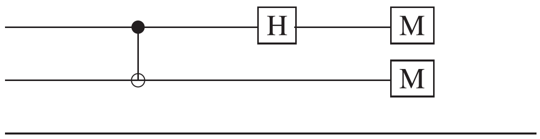
Finally, B does a phase flip on his qubit, yielding

$$\sum_j a_j \big| j, j \big\rangle.$$

This is almost exactly what we want. The only problem is that now, the qubit corresponding to $|\psi\rangle$ is entangled with B's qubit. The entanglement that was necessary to get the whole process started is now a liability. One way to disentangle them would be for A to measure her remaining qubit. But this would destroy B's qubit as well.

The ideal solution would be to send the entangle qubits through a CNOT gate—but A controls the first qubit and B controls the second. This would require quantum communication between A and B, which is prohibited.

The correct solution is to go back and modify the original diagram, inserting a Hadamard gate and an additional measurement:



Now the algorithm proceeds exactly as before. However A's application of the Hadamard gate now induces the transformation

$$\sum_j a_j\big|j,j\big\rangle \longrightarrow \sum_{ij} a_j(-1)^{ij}\big|i,j\big\rangle.$$

Finally A measures i and sends the measurement to B. The state is now:

$$\sum_j a_j(-1)^{ij}|j\rangle.$$

If $i = 0$ then we are done; if $i = 1$ then B applies a phase flip. In either case the state is now $a_0|0\rangle + a_1|1\rangle$.

So A has transported the quantum state to B simply by sending two classical bits.