CS 294-2 Hilbert Spaces, Tensor Products, Quantum Gates, Bell States 1/22/07
Spring 2007 Lecture 2

0.1 Hilbert Spaces

Consider a discrete quantum system that has k distinguishable states (e.g. k distinct energy states of the electron in a Hydrogen atom). The state of such a system is a unit vector in a k dimensional complex vector space $\mathscr{C}^k$. The k distinguishable states form an orthogonal basis for the vector space - denoted by, say, $\{|1\rangle, \ldots, |k\rangle$. Here we are using the standard inner-product over $\mathscr{C}^k$ to define orthogonality. Recall that the inner-product of two vectors $|\phi\rangle = \sum_i \alpha_i |i\rangle$ and $|\psi\rangle = \sum_i \beta_i |i\rangle$ is $\sum_i \bar{\alpha}_i \beta_i$.

Dirac's Bra-ket Notation

We have already introduced the ket notation for vectors. We denote by $\langle\phi|$ (pronounced *bra*(ϕ)) the row vector $(\overline{\alpha_1} \cdots \overline{\alpha_k})$. i.e. the conjugate transpose of $|\phi\rangle$. In this notation, the inner-product of $|\phi\rangle$ and $|\psi\rangle$ is just $\langle\phi|\,|\psi\rangle$.

To demonstrate the utility of this notation, let $|v\rangle$ be a vector of norm 1. Define $P = |v\rangle\langle v|$. Then for any $|w\rangle$ we have $P|w\rangle = |v\rangle\langle v|w\rangle$, so P is the projection operator onto $|v\rangle$ (see diagram.) Note that $P^2 = |v\rangle\langle v|v\rangle\langle v| = P$ since $|v\rangle$ has norm 1.

More abstractly, the state of a quantum system is a unit vector in a Hilbert space. A Hilbert space is a complex vector space endowed with an inner-product and which is complete under the induced norm. The last condition will not be of much concern for us since we will mostly be concerned with finite dimensional Hilbert spaces.

0.2 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

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

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

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

0.3 The Significance of Tensor Products

Classically, if we put together a subsystem that stores k bits of information with one that stores l bits of information, the total capacity of the composite system is $k+l$ bits. Or put another way, if k bits of information are required to describe the state of the first subsystem and l bits to describe the second, then $k+l$ bits suffice to describe the composite system.

From this viewpoint, the situation with quantum systems is extremely paradoxical. We need k complex numbers to describe the state of a k-level quantum system. Now consider a system that consists of a k-level subsystem and an l-level subsystem. To describe the composite system we need kl complex numbers. If the state of the system was known to be a tensor product state $|\phi\rangle \otimes |\psi\rangle$ then only $k+l$ complex numbers would suffice. It follows that most states of the composite system are not tensor product states. They are entangled states. This brings up another question: one might wonder where nature finds the extra storage space when we put these two subsystems together.

An extreme case of this phenomenon occurs when we consider an n qubit quantum system. The Hilbert space associated with this system is the n-fold tensor product of $\mathscr{C}^2 \equiv \mathscr{C}^{2^n}$. Thus nature must "remember" of 2^n complex numbers to keep track of the state of an n qubit system. For modest values of n of a few hundred, 2^n is larger than estimates on the number of elementary particles in the Universe.

This is the fundamental property of quantum systems that is used in quantum information processing.

Finally, note that when we actually a measure an n-qubit quantum state, we see only an n-bit string - so we can recover from the system only n, rather than 2^n, bits of information.

0.4 Unitary Operators

The final postulate of quantum physics states that the evolution of a quantum system is necessarily unitary. Intuitively, a unitary transformation is a rigid body rotation (or reflection) of the Hilbert space, thus resulting in a transformation of the state vector that doesn't change its length.

Suppose we have a k-state quantum system. Then a unitary transformation over the space is a linear transformation that can be specified by a $k \times k$ matrix U with complex entries that satisfies $U^{-1} = U^\dagger$. For example, for an op erator on $\mathscr{C}^2$,

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow U^\dagger = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \quad .$$

It is easily verified that the composition of two unitary transformations is also unitary (Proof: U, V unitary, then $(UV)^\dagger = V^\dagger U^\dagger = V^{-1}U^{-1} = (UV)^{-1}$).

Some properies of a unitary transformation U:

- The rows of U form an orthonormal basis.
- The columns of U form an orthonormal basis.

- U preserves inner products, i.e. the inner product between $|u\rangle$ and $|v\rangle$ is the same as the inner product between $U|u\rangle$ and $U|v\rangle$. The latter quantity can be written as $\langle v|U^{\dagger}U|w\rangle = \langle v|w\rangle$. Therefore, U preserves norms and angles (up to sign).
- The eigenvalues of U are all of the form $e^{i\theta}$ (since U is length-preserving, i.e., $(\vec{v},\vec{v}) = (U\vec{v},U\vec{v})$).
- U can be diagonalized into the form

$$\begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & e^{i\theta_k} \end{pmatrix}$$

0.5 Quantum Gates

We give some examples of simple unitary transforms, or "quantum gates."

Some quantum gates with one qubit:

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$, or a rotation around $\pi/4$ followed by a reflection.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

  The Hadamard Gate is one of the most important gates. Note that $H^{\dagger} = H$ – since H is real and symmetric – and $H^2 = I$.

- Rotation Gate. This rotates the plane by θ.

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

- NOT Gate. This flips a bit from 0 to 1 and vice versa.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase Flip.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  The phase flip is a NOT gate acting in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis. Indeed, $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

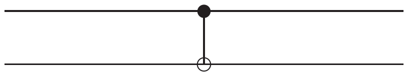
And a two-qubit quantum gate:

- Controlled Not (CNOT).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

  The first bit of a CNOT gate is the "control bit;" the second is the "target bit." The control bit never changes, while the target bit flips if and only if the control bit is 1.

  The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



0.6 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 $0 \leq i \leq k-1$ and $0 \leq j \leq l-1$. 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.

0.7 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:

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

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

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

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

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 Bell's Inequality

Let us return to the proof of the Bell inequality from last time. The experiment we described there was the following:

Alice and Bob share a Bell state, say $|Phi^+\rangle$. Alice is given as input a random bit x_A and Bob a random bit x_B. Alice applies a rotation of $-\pi/16$ to her qubit if $x_A = 0$ and $3\pi/6$ if $x_A = 1$. Bob applies a rotation of $\pi/16$ to his qubit if $x_B = 0$ and $-3\pi/6$ if $x_B = 1$. Both then measure their qubits in the standard basis and output their results.

We wish to determine the probability of the event $x_A \cdot x_B = a + b \bmod 2$.

To make the calculation easier, assume instead that Alice and Bob share the Bell state Ψ^-, and Bob outputs the complement of the bit that he measures. Now, by the rotational symmetry of Ψ^-, it follows that if Alice rotates by α and Bob by β, then the probability that they measure different values (and therefore output the same value) is $cos^2(\alpha - \beta)$. In the three cases where $x_A \cdot x_B = 0$, $|\alpha - \beta| = \pi/8$, and so the chance that $a = b$ or $a + b = 0 \bmod 2$ is $cos^2\pi/8$. In the case that where $x_A \cdot x_B = 1$, $|\alpha - \beta| = 3\pi/8$. But now the chance that $a \neq b$ or $a + b = 1 \bmod 2$ is $sin^2 3\pi/8 = cos^2\pi/8$. Therefore in all four cases the chance that $x_A \cdot x_B = a + b \bmod 2$ is $cos^2\pi/8$.