This lecture will formalize many of the notions introduced informally in the second lecture.

1 Hilbert Spaces

Consider a discrete quantum system that has $k$ distinguishable states (e.g. a system that can be in one of $k$ distinct energy states. The state of such a system is a unit vector in a $k$ dimensional complex vector space $\mathbb{C}^k$. The $k$ distinguishable states form an orthogonal basis for the vector space - say denoted by $\{|1\rangle, \ldots, |k\rangle\}$. Here we are using the standard inner-product over $\mathbb{C}^k$ 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 $\sum_i \overline{\alpha}_i \beta_i$.

Dirac’s Braket Notation

We have already introduced the ket notation for vectors. If $|v\rangle = \sum_i \alpha_i |i\rangle$ and $|w\rangle = \sum_i \beta_i |i\rangle$, then we have already observed that

$$ (\vec{v}, \vec{w}) = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_d \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_d \end{pmatrix}. $$

We denote the row vector $(\alpha_1 \cdots \alpha_d)$ by $\langle v |$ and the inner product $(\vec{v}, \vec{w})$ by $\langle v | w \rangle$.

$\langle v |$ is a bra, and $|w\rangle$ is a ket, so $\langle v | w \rangle$ is a braket.

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 $P^2 = |v\rangle \langle v | v \rangle = P$ 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 vector space axioms give us notions of span and linear independence of a set of vectors. However, to endow the vector space with geometry — the notion of angle between two vectors and the norm or length of a vector, we must define an inner-product — whose properties are listed below. The third property — completeness — is trivially satisfied for a finite dimensional system, so we will not bother to define it here.

- An inner product on a (complex) vector space $V$ is a map $(\cdot, \cdot) : V \times V \rightarrow \mathbb{C}$ satisfying for each $\vec{u}, \vec{v}, \vec{w} \in V$ and $\alpha, \beta \in \mathbb{C}$:
  
  (i) $(\vec{u}, \vec{v}) \geq 0$, and $(\vec{v}, \vec{v}) = 0$ if and only if $\vec{v} = \vec{0}$;
  
  (ii) $(\alpha \vec{u} + \beta \vec{v}, \vec{w}) = \alpha (\vec{u}, \vec{w}) + \beta (\vec{v}, \vec{w})$;
  
  (iii) $(\vec{u}, \vec{w}) = (\vec{w}, \vec{u})$.  

An inner product space is a vector space together with an inner product.

- Vectors \( \vec{v}, \vec{w} \in V \) are orthogonal if \((\vec{v}, \vec{w}) = 0\).

- A basis for \( V \) is a set \( \{\vec{v}_1, \cdots, \vec{v}_d\} \) such that each \( \vec{v} \in V \) can be written uniquely in the form \( \vec{v} = \alpha_1 \vec{v}_1 + \cdots + \alpha_d \vec{v}_d \). The basis is said to be orthonormal if \((\vec{v}_i, \vec{v}_j) = \delta_{ij} \) for each \( i, j \). (Here \( \delta_{ij} = 1 \) if \( i = j \) and 0 if \( i \neq j \).)

Note that we can associate to each inner product space a canonical norm, defined by \( \|\vec{v}\| = \sqrt{(\vec{v}, \vec{v})} \). A Hilbert space is an inner product space which is complete with respect to its norm. If \( V \) is finite-dimensional (i.e. it has a finite basis), then completeness is automatically satisfied. Furthermore, there is only one Hilbert space of each dimension (up to isomorphism.)

2 Tensor Products

Consider two quantum systems - the first with \( k \) distinguishable (classical) states (associated Hilbert space \( \mathbb{C}^k \)), and the second with \( l \) distinguishable states (associated Hilbert space \( \mathbb{C}^l \)). 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 \( \mathbb{C}^{kl} \).

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

\[
(\langle|v_1\rangle \otimes |w_1\rangle, |v_2\rangle \otimes |w_2\rangle) = (|v_1\rangle, |v_2\rangle) \cdot (|w_1\rangle, |w_2\rangle),
\]

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

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

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

A word of caution: Not all elements of \( V \otimes W \) can be written as \( |v\rangle \otimes |w\rangle \) for \( |v\rangle \in V, |w\rangle \in W \). As an example, consider the Bell state \( |\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \).
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.

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. 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 $\mathbb{C}^2 \equiv \mathbb{C}^{2^n}$. 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.

4 Unitary Operators and Quantum Gates

4.1 Unitary Operators

A postulate of quantum physics is that quantum evolution is unitary. That is, if we have some arbitrary quantum system $U$ that takes as input a state $|\phi\rangle$ and outputs a different state $U|\phi\rangle$, then we can describe $U$ as a unitary linear transformation, defined as follows.

If $U$ is any linear transformation, the adjoint of $U$, denoted $U^\dagger$, is defined by $(U\vec{v},\vec{w}) = (\vec{v},U^\dagger\vec{w})$. In a basis, $U^\dagger$ is the conjugate transpose of $U$; for example, for an operator on $\mathbb{C}^2$,

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

We say that $U$ is unitary if $U^\dagger = U^{-1}$. For example, rotations and reflections are unitary. Also, 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 properties 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. $(\vec{v},\vec{w}) = (U\vec{v},U\vec{w})$. Indeed, $(U\vec{v},U\vec{w}) = (U|v\rangle \langle w|U^\dagger = \langle v|U^\dagger U|w\rangle = \langle v|w\rangle$. 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

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

4.2 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 $\theta$.

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

• 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:

```
```

4
4.3 Tensor product of operators

Suppose $|v\rangle$ and $|w\rangle$ are unentangled states on $\mathbb{C}^m$ and $\mathbb{C}^n$, respectively. The state of the combined system is $|v\rangle \otimes |w\rangle$ on $\mathbb{C}^{mn}$. 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, $(A \otimes B)(|0\rangle \otimes |0\rangle) = A|0\rangle \otimes B|0\rangle$. Therefore, we define $(A \otimes B)(|0\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(A \otimes B)|0\rangle + \frac{1}{\sqrt{2}}(A \otimes B)|1\rangle = \frac{1}{\sqrt{2}}(A|0\rangle \otimes B|0\rangle + A|1\rangle \otimes B|1\rangle)$.)

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 $i,j$th 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

\[
A \otimes B = \left( \sum_{ij} a_{ij} |e_i\rangle \langle e_j| \right) \otimes \left( \sum_{kl} b_{kl} |f_k\rangle \langle f_l| \right) = \sum_{ijkl} a_{ij} b_{kl} |e_i\rangle \langle e_j| \otimes |f_k\rangle \langle f_l| = \sum_{ijkl} a_{ij} b_{kl} (|e_i\rangle \otimes |f_k\rangle)(\langle e_j| \otimes \langle f_l|).
\]

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 $i, j$th subblock, we multiply $a_{ij}$ by the matrix for $B$. 