1 More on Measurements

Recall that the state of a single qubit can be written as a superposition over the possibilities 0 and 1: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Measuring in the standard basis, then, there is probability $|\alpha|^2$ that we get 0 and the new state is $|\psi'\rangle = |0\rangle$, and probability $|\beta|^2$ that we get 1 and $|\psi'\rangle = |1\rangle$.

A measurement can be written as a projector. A projector $P_i = |i\rangle\langle i|$ takes a ket $|\psi\rangle$ and replaces it by its component $|i\rangle$, with amplitude $\langle i||\psi\rangle$. The spectral resolution of the identity defines a set of projectors. For a general expansion $|\psi\rangle = \sum_j c_j|j\rangle$ and an orthonormal basis $\{|i\rangle\}$, we have the corresponding resolution of the identity:

$$I = \sum_i |i\rangle\langle i| = \sum_i P_i$$

E.g., $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ for a two state basis.

Hence

$$P_i|\psi\rangle = |i\rangle\langle i|\psi\rangle = \sum_j c_j\langle i|j\rangle|j\rangle = \sum_j \delta_{i,j}c_j|i\rangle = c_i|i\rangle$$

Note: operators may generally be written in the form $O = \{\langle a|b\rangle\}_{\{a,b\}}$.

More generally, we can measure the qubit in any orthonormal basis simply by projecting $|\psi\rangle$ onto the two basis vectors. See Figure 1.

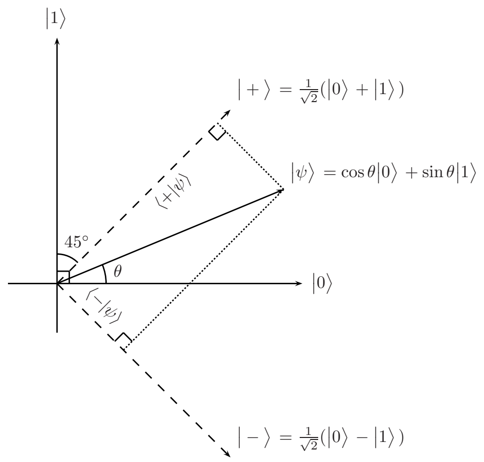
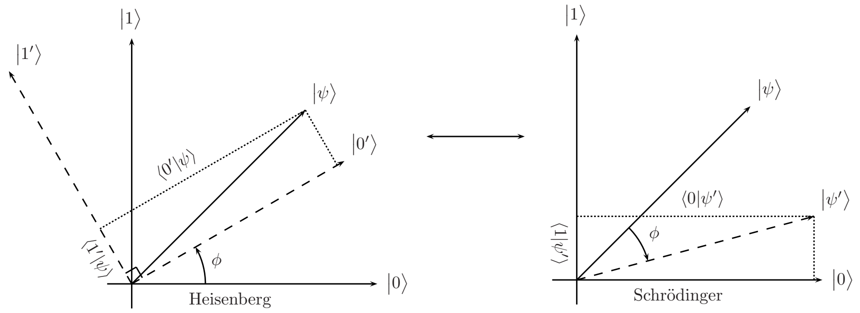


Figure 1:

The new state of the system $|\psi'\rangle$ is the outcome of the measurement. Alternatively, instead of measuring the system in a rotated basis, we rotate the system (in the opposite direction) and measure it in the original, standard basis.



2 One-qubit Unitaries/Gates

Rotations over a complex vector space are called unitary transformations. For example, rotation by θ is unitary. Reflection about the line $\theta/2$ is also unitary. Unitary operations U satisfy

$$UU^\dagger = U^\dagger U = 1$$

i.e., $U^\dagger = U^{-1}$, the adjoint of the operator is equal to its inverse. (Recall that in the matrix representation we have $[U^\dagger]_{ij} = [U^*_{ji} = [U^T]^*_{ij})$

One very important unitary is the time evolution operator

$$U = exp(-iHt)$$

where H is the Hamiltonian operator of the quantum system. In computer science we usually analyze quantum operations in terms of unitaries, or "gates". To physically realize these gates we need to implement the corresponding Hamiltonian operators H.

In order to manipulate a qubit, we must manipulate its state:

$$|\psi >= \alpha|0> + \beta|1>$$

This is done by acting on $|\psi>$ with unitary operators (i.e. gates) such that

$$\hat{U}|\psi >= \alpha'|0> + \beta'|1>$$

where $\hat{U}$ is a 2×2 unitary matrix.

Hadamard gate:

The Hadamard gate is a reflection about the line $\theta = \pi/8$. This reflection maps the x-axis to the 45° line, and the y-axis to the $-45°$ line. That is

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \equiv |+\rangle \tag{1}$$

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \equiv |-\rangle \quad . \tag{2}$$

In matrix form, we write

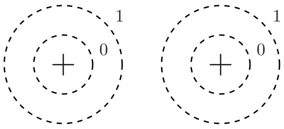
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad .$$

Notice that, starting in $|\psi\rangle$ either $|0\rangle$ or $|1\rangle$, $H|\psi\rangle$ when measured is equally likely to give 0 and 1. There is no longer any distinguishing information in the bit. This information has moved to the phase (in the computational basis).

In a quantum circuit diagram, we imagine the qubit travelling from left to right along the wire. The following diagram shows the application of a Hadamard gate.

3 Two qubits

Now let us examine the case of two qubits. Consider the two electrons in two hydrogen atoms:



Since each electron can be in either of the ground or excited state, classically the two electrons are in one of four states – 00, 01, 10, or 11 – and represent 2 bits of classical information. Quantum mechanically, they are in a superposition of those four states:

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

where $\sum_{ij} |\alpha_{ij}|^2 = 1$. Again, this is just Dirac notation for the unit vector in $\mathscr{C}^4$:

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

where $\alpha_{ij} \in \mathscr{C}$, $\sum |\alpha_{ij}|^2 = 1$.

Measurement:

If the two electrons (qubits) are in state $|\psi\rangle$ and we measure them, then the probability that the first qubit is in state i, and the second qubit is in state j is $P(i,j) = |\alpha_{ij}|^2$. Following the measurement, the state of the two qubits is $|\psi'\rangle = |ij\rangle$. What happens if we measure just the first qubit? What is the probability that the first qubit is 0? In that case, the outcome is the same as if we had measured both qubits: $\Pr\{\text{1st bit } = 0\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. The new state of the two qubit system now consists of those terms in the superposition that are consistent with the outcome of the measurement – but normalized to be a unit vector:

$$|\phi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

.

A more formal way of describing this partial measurement is that the state vector is projected onto the subspace spanned by $|00\rangle$ and $|01\rangle$ with probability equal to the square of the norm of the projection, or onto the orthogonal subspace spanned by $|10\rangle$ and $|11\rangle$ with the remaining probability. In each case, the new state is given by the (normalized) projection onto the respective subspace.

Tensor products (informal):

Suppose the first qubit is in the state $|\phi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and the second qubit is in the state $|\phi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$. How do we describe the joint state of the two qubits?

$$\begin{aligned} |\phi\rangle &= |\phi_1\rangle \otimes |\phi_2\rangle \\ &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle \ . \end{aligned}$$

We have simply multiplied together the amplitudes of $|0\rangle_1$ and $|0\rangle_2$ to determine the amplitude of $|00\rangle_{12}$, and so on. The two qubits are not entangled with each other and measurements of the two qubits will be distrbuted independently.

Given a general state of two qubits can we say what the state of each of the individual qubits is? The answer is usually no. For a random state of two qubits is entangled — it cannot be decomposed into state of each of two qubits. In the next lecture we will study the Bell states, which are maximally entangled states of two qubits.

4 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 $\mathscr{C}^k$. 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 $\mathscr{C}^k$ 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 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

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

We denote the row vector $(\overline{\alpha_1} \cdots \overline{\alpha_d})$ 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 $P^2 = |v\rangle\langle v|v\rangle\langle v| = P$ 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 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 $(\cdot,\cdot) : V \times V \to \mathscr{C}$ satisfying for each $\vec{u},\vec{v},\vec{w} \in V$ and $\alpha, \beta \in \mathscr{C}$:

  (i) $(\vec{v},\vec{v}) \geq 0$, 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) $(\vec{v},\vec{w}) = \overline{(\vec{w},\vec{v})}$.

  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 $\vec{v} = \alpha_1\vec{v}_1+\cdots+\alpha_n\vec{v}_n$. 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.)

5 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

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

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

5.1 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 $\mathscr{C}^2 \equiv \mathscr{C}^{2^n}$. 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.