Unitary time evolution

- Time evolution of quantum systems is always given by *Unitary Transformations*. If the state of a quantum system is $|\psi\rangle$, then at a later time

$$|\psi\rangle \to \hat{U}|\psi\rangle.$$

  Exactly what this operator $\hat{U}$ is will depend on the particular system and the *interactions* that it undergoes. It does not, however, depend on the state $|\psi\rangle$. This means that time evolution of quantum systems is *linear*.

- Because of this linearity, if a system is in state $|\psi\rangle$ or $|\phi\rangle$ or any linear combination, the time evolution is given by the same operator:

$$(\alpha|\psi\rangle + \beta|\phi\rangle) \to \hat{U}(\alpha|\psi\rangle + \beta|\phi\rangle) = \alpha\hat{U}|\psi\rangle + \beta\hat{U}|\phi\rangle.$$

The Schrödinger equation

As we have seen, these unitary operators arise from the *Schrödinger equation*

$$d|\psi\rangle/dt = -i\hat{H}(t)|\psi\rangle/\hbar,$$

where $\hat{H}(t) = \hat{H}^\dagger(t)$ is the *Hamiltonian* of the system. Because this is a linear equation, the time evolution must be a linear transformation. We can prove that this must be a unitary transformation very simply.

Suppose $|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle$ for some matrix $\hat{U}(t)$ (which we don't yet assume to be unitary). Plugging this into the Schrödinger equation gives us:

$$\frac{d\hat{U}(t)}{dt} = -i\hat{H}(t)\hat{U}(t)/\hbar, \quad \frac{d\hat{U}^\dagger(t)}{dt} = i\hat{U}^\dagger(t)\hat{H}(t)/\hbar.$$

At $t = 0$, $\hat{U}(0) = \hat{I}$, so $\hat{U}^\dagger(0)\hat{U}(0) = \hat{I}$. We see that

$$\frac{d}{dt}\left(\hat{U}^\dagger(t)\hat{U}(t)\right) = \frac{1}{\hbar}\hat{U}^\dagger(t)\left(i\hat{H}(t) - i\hat{H}(t)\right)\hat{U}(t) = 0.$$

So $\hat{U}^\dagger(t)\hat{U}(t) = \hat{I}$ at all times t, and $\hat{U}(t)$ must always be unitary.

For time-independent Hamiltonians we can easily write down the solution to the Schrödinger equation. Using the spectral theorem, we choose a basis $\{|k\rangle\}$ of *eigenvectors* of $\hat{H}$ with eigenvalues E_k, $\hat{H}|k\rangle = E_k|k\rangle$. We then write $|\psi(t)\rangle$ in terms of this basis:

$$\hat{H} = \sum_k E_k |k\rangle\langle k|, \quad |\psi(t)\rangle = \sum_k \alpha_k(t)|k\rangle, \quad \sum_k |\alpha_k(t)|^2 = 1.$$

Knowing $|\psi(t)\rangle = \exp(-i\hat{H}t/\hbar)|\psi(0)\rangle$ for any t means knowing the amplitudes $\alpha_k(t)$. From the Schrödinger equation,

$$\frac{d\alpha_k}{dt} = -iE_k\alpha_k/\hbar \implies \alpha_k(t) = \exp(-iE_kt/\hbar)\alpha_k(0).$$

Each energy eigenstates undergoes a *steady phase rotation*.

Bloch sphere rotation

Any 2×2 Hermitian operator can be written $\hat{H} = a\hat{I} + b\hat{X} + c\hat{Y} + d\hat{Z}$ with real a, b, c, d. Spin-1/2 unitaries take the form

$$\hat{U}(t) = \exp\left(-(it/\hbar)(a\hat{I} + b\hat{X} + c\hat{Y} + d\hat{Z})\right)$$

We now need to use a very useful and important fact. For general operators $\hat{A}$ and $\hat{B}$, usually

$$\exp(\hat{A})\exp(\hat{B}) \neq \exp(\hat{A} + \hat{B}).$$

The one exception to this is when $[\hat{A}, \hat{B}] = 0$. In this case only, $\exp(\hat{A})\exp(\hat{B}) = \exp(\hat{A} + \hat{B})$.

Since the identity commutes with everything,

$$\exp\left(-\frac{it}{\hbar}\left(a\hat{I} + b\hat{X} + c\hat{Y} + d\right)\right)$$

$$= \exp\left(-\frac{iat}{\hbar}\hat{I}\right)\exp\left(-\frac{it}{\hbar}\left(b\hat{X} + c\hat{Y} + d\hat{Z}\right)\right)$$

$$= e^{-iat/\hbar}\exp\left(-(it/\hbar)(b\hat{X} + c\hat{Y} + d\hat{Z})\right).$$

Since an overall phase is meaningless, we can always set $a = 0$. (This is not just true for spin-1/2; one can add or subtract a term $a\hat{I}$ to any Hamiltonian.)

The most general spin-1/2 Hamiltonian is therefore

$$\hat{H} = b\hat{X} + c\hat{Y} + d\hat{Z} = E_0\vec{n}\cdot\hat{\vec{\sigma}}$$

where

$$E_0 = \sqrt{b^2 + c^2 + d^2},$$

$$\vec{n} = (n_x, n_y, n_z) = (b/E_0, c/E_0, d/E_0),$$

with $n_x^2 + n_y^2 + n_z^2 = 1$ and $\hat{\vec{\sigma}} = (\hat{X}, \hat{Y}, \hat{Z})$. The unitary is

$$\exp(-i\hat{H}t/\hbar) = \cos(E_0 t/\hbar)\hat{I} - i\sin(E_0 t/\hbar)\vec{n}\cdot\hat{\vec{\sigma}}.$$

In the Bloch sphere picture this corresponds to a rotation around the axis $\vec{n}$ at a rate $E_0/\hbar$. This is the most general unitary transformation possible for spin-1/2.

Controlling unitaries

We generalize from steady rotation by assuming we can turn the Hamiltonian on and off. By turning a Hamiltonian on for a particular length of time, we can “rotate” the state by a particular angle. For a spin-1/2, this means we can perform unitary transformations of the form

$$\hat{U}(\theta) = \cos(\theta/2)\hat{I} - i\sin(\theta/2)\vec{n}\cdot\hat{\vec{\sigma}}.$$

We can do the same with more complicated systems. For a D-dimensional system with a Hamiltonian $\hat{H}$ having eigenvalues E_k and eigenvectors $|k\rangle$, we can do the unitary

$$\hat{U}(\tau) = \sum_k \exp(-iE_k\tau/\hbar)|k\rangle\langle k|$$

for any τ.

Building up unitaries

Unfortunately, we cannot always choose the exact values of the eigenvalues E_k or the eigenvectors $|k\rangle$. These are generally given to us by nature. But we sometimes can increase the range of our options by *combining* several different unitaries in a row. The important thing to remember is that any *product* of unitary operators is *also* unitary:

$$\hat{U}^\dagger \hat{U} = \hat{V}^\dagger \hat{V} = \hat{I} \implies (\hat{U}\hat{V})^\dagger (\hat{U}\hat{V}) = \hat{V}^\dagger \hat{U}^\dagger \hat{U}\hat{V} = \hat{I}.$$

Suppose there are two *different* Hamiltonians we can turn on: $\hat{H}_1$ and $\hat{H}_2$. Then we can perform the unitaries

$$\hat{U}_1(\tau) = \exp(-i\hat{H}_1\tau/\hbar), \quad \hat{U}_2(\tau) = \exp(-i\hat{H}_2\tau/\hbar).$$

But we can do much more than these!

We can *also* do the unitaries

$$\hat{U}_2(\tau_2)\hat{U}_1(\tau_1), \quad \text{and} \quad \hat{U}_2(\tau_3)\hat{U}_1(\tau_2)\hat{U}_2(\tau_1),$$

$$\text{and} \quad \hat{U}_2(\tau_n)\hat{U}_1(\tau_{n-1})\cdots\hat{U}_2(\tau_2)\hat{U}_1(\tau_1).$$

Let's see how this works for the spin-1/2. Suppose we can turn on Hamiltonians

$$\hat{H}_1 = E_x\hat{X}, \quad \hat{H}_2 = E_y\hat{Y}.$$

These produce unitaries $\hat{U}_1(\theta)$ and $\hat{U}_2(\theta)$ which correspond, in the Bloch sphere representation, to rotations by θ about the X and Y axes, respectively.

- There is a theorem in geometry that a rotation by any angle θ around any axis $\vec{n}$ can be done by doing three rotations in a row around the X and Y axes:

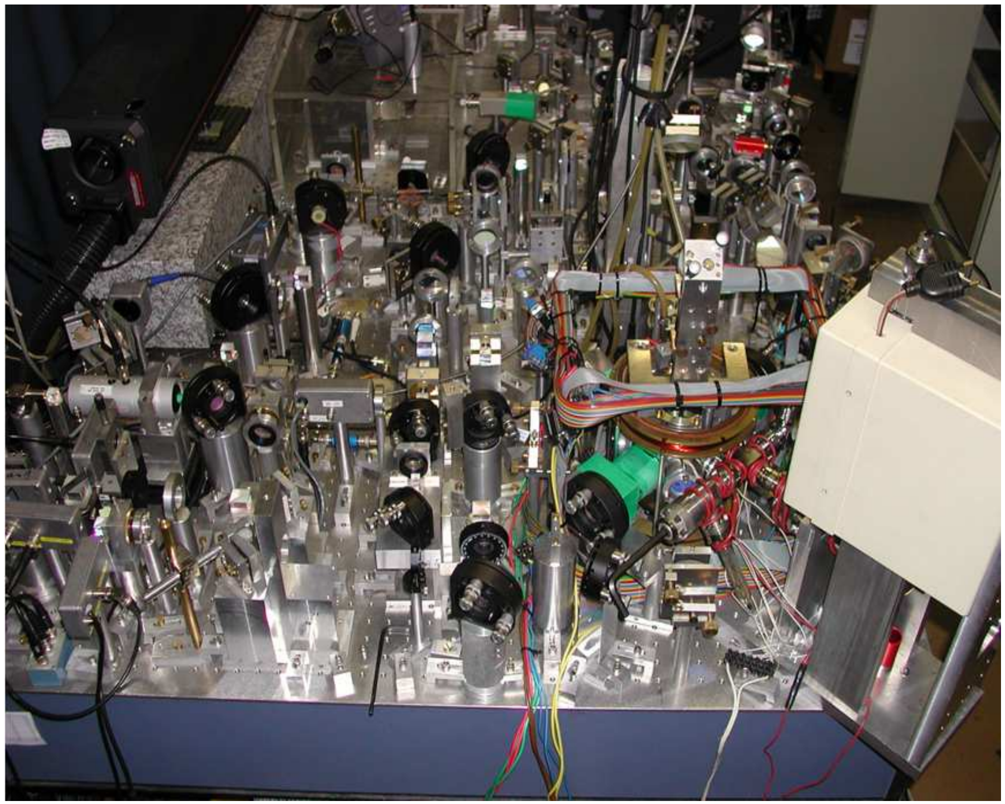
$$R_{\vec{n}}(\theta) = R_X(\phi_3)R_Y(\phi_2)R_X(\phi_1)$$

  for some ϕ_1, ϕ_2, ϕ_3.
- Since every 2×2 unitary is equivalent to a Bloch sphere rotation about some axis $\vec{n}$, any 2×2 unitary equals

$$\hat{U}_X(\tau_3)\hat{U}_Y(\tau_2)\hat{U}_X(\tau_1)$$

  for some τ_1, τ_2, τ_3 (up to an overall phase).
- When we talk about "turning on" and "turning off" Hamiltonians, what do we really mean?

Here is a picture to give some idea:



For many experimental systems, unitaries are effected by turning precisely-tuned lasers on and off for precise lengths of time.

Tensor products of unitaries

We have seen that Hilbert spaces of *composite* systems are represented by *tensor products* of the Hilbert spaces of the component systems:

$$\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2.$$

Therefore, unitaries on the joint system also act on this larger Hilbert space. Suppose that the Hamiltonian of a system is a sum of terms which act only on the individual subsystems:

$$\hat{H} = \hat{H}_1 \otimes \hat{I} + \hat{I} \otimes \hat{H}_2.$$

The two terms represent the Hamiltonian of the first and second subsystems, respectively. In this Hamiltonian, the two subsystems are isolated, and do not interact.

- $\hat{H}_1 \otimes \hat{I}$ and $\hat{I} \otimes \hat{H}_2$ commute, so

$$\begin{aligned}
\hat{U}(t) &= \exp(-i\hat{H}t/\hbar) \\
&= \exp(-i(\hat{H}_1 \otimes \hat{I} + \hat{I} \otimes \hat{H}_2)t/\hbar) \\
&= \exp(-i\hat{H}_1 \otimes \hat{I}t/\hbar)\exp(-i\hat{I} \otimes \hat{H}_2 t/\hbar) \\
&= \exp(-i\hat{H}_1 t/\hbar) \otimes \exp(-i\hat{H}_2 t/\hbar) \\
&\equiv \hat{U}_1(t) \otimes \hat{U}_2(t).
\end{aligned}$$

  It is a tensor product of unitaries.

- What if the Hamiltonian is *not* a sum of terms which act on the individual subsystems, but includes terms which act on *both* subsystems?

Interactions and entanglement

- If the Hamiltonian has the form

$$\hat{H} = \hat{H}_1 \otimes \hat{I} + \hat{I} \otimes \hat{H}_2 + \hat{H}_{\rm int},$$

  the unitary $\hat{U}(t) = \exp(-i\hat{H}t/\hbar)$ will not be a tensor product, in general. In this case, we say that the two subsystems *interact*.

- If a tensor-product unitary $\hat{U}_1 \otimes \hat{U}_2$ acts on a product state $|\psi\rangle \otimes |\phi\rangle$, then it will remain a product state. If a general $\hat{U}$ acts on it, generally the state becomes *entangled*. Since most states are entangled, to produce them from initial product states requires unitaries which are not products. *We must have interactions between the subsystems to produce general unitary transformations.*

Let's take an example for two spin-1/2s: $\hat{H}_{\rm int} = E_{\rm int}\hat{Z} \otimes \hat{Z}$. This yields unitary transformations of the form

$$\hat{U}(\theta) = \cos(\theta/2)\hat{I} - i\sin(\theta/2)\hat{Z} \otimes \hat{Z}.$$

Suppose we have an initial product state $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$

$$= \alpha_1\beta_1|\uparrow\uparrow\rangle + \alpha_1\beta_2|\uparrow\downarrow\rangle + \alpha_2\beta_1|\downarrow\uparrow\rangle + \alpha_2\beta_2|\downarrow\downarrow\rangle.$$

When we transform it by $\hat{U}(\theta)$ it becomes

$$\begin{aligned}\hat{U}(\theta)|\Psi\rangle &= e^{-i\theta/2}\alpha_1\beta_1|\uparrow\uparrow\rangle + e^{i\theta/2}\alpha_1\beta_2|\uparrow\downarrow\rangle \\ &\quad + e^{i\theta/2}\alpha_2\beta_1|\downarrow\uparrow\rangle + e^{-i\theta/2}\alpha_2\beta_2|\downarrow\downarrow\rangle,\end{aligned}$$

which is no longer a product state for $\theta \neq m\pi/2$. The interaction has produced entanglement.

The no-cloning theorem

- The restriction of time evolution to unitary operators means that certain kinds of evolution are *impossible*. One impossible task is *quantum cloning*.
- Suppose we have a system in an unknown state $|\psi\rangle$, and we wish to *copy* it, i.e., to transform a second system starting in some standard state $|0\rangle$ into the same state $|\psi\rangle$. Is there a unitary $\hat{U}$ such that, for any state $|\psi\rangle$,

$$\hat{U}\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle ?$$

- If this is true, then also for $|\phi\rangle \neq |\psi\rangle$

$$\hat{U}\left(|\phi\rangle \otimes |0\rangle\right) = |\phi\rangle \otimes |\phi\rangle .$$

- Consider now a superposition state $|\chi\rangle = \alpha|\psi\rangle + \beta|\phi\rangle$. By linearity,

$$\begin{aligned}\hat{U}(|\chi\rangle \otimes |0\rangle) &= \hat{U}(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes |0\rangle \\ &= \alpha|\psi\rangle \otimes |\psi\rangle + \beta|\phi\rangle \otimes |\phi\rangle \\ &\neq (\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle),\end{aligned}$$

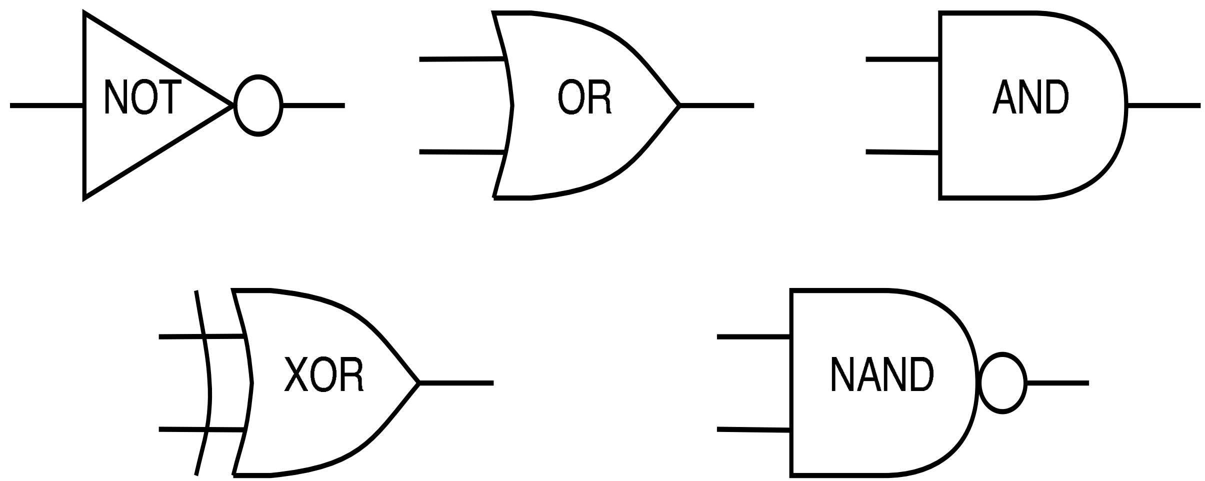
so $\hat{U}(|\chi\rangle \otimes |0\rangle) \neq |\chi\rangle \otimes |\chi\rangle$, which is a contradiction. Therefore, no such $\hat{U}$ exists.

- This is the famous *no-cloning theorem*: quantum information, unlike classical information, *cannot be copied*.

- This simple result has many profound consequences. For one, *the state $|\psi\rangle$ of a system is not an observable*. Given a quantum system, there is no way to tell in what state $|\psi\rangle$ it was prepared.
- If the state $|\psi\rangle$ is *known*, the state can be “copied” by preparing another system. But it is impossible to copy an *unknown* quantum state.
- This means that many techniques of classical information theory (such as protecting information by making redundant copies, or having a *fanout* gate from a single bit) are impossible in quantum information theory.

Quantum gates and circuits

We have seen that it is possible to build up new unitary operators by multiplying together some set of standard ones. This is rather analogous to the situation in classical logic, where *any* Boolean function can be built up from a set of standard functions of one or two bits, called logical *gates*:



We can similarly try to build up unitary transformations from a set of standard unitaries. We will call these *quantum gates*.

- First we define the basic unit of quantum information: the *quantum bit*. This is the simplest possible quantum system, one with two distinguishable states. In other words, the quantum bit (or *q-bit*) is our old friend, the spin-1/2! We take the standard basis to be $|0\rangle \equiv |\uparrow_Z\rangle$, $|1\rangle \equiv |\downarrow_Z\rangle$.
- The simplest gate, affecting only a single q-bit, is the *NOT* gate:

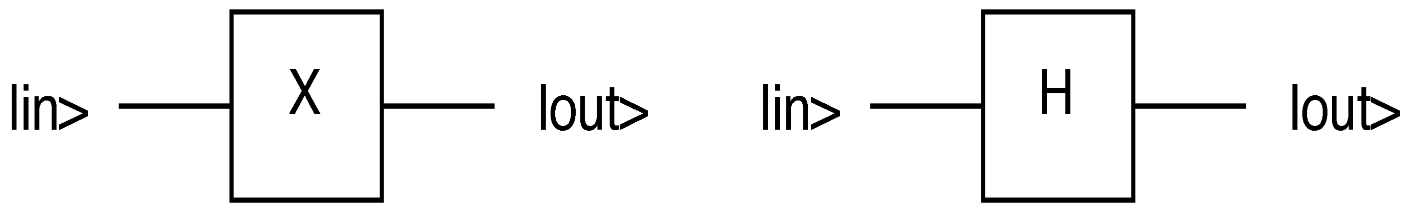
  $$|0\rangle \leftrightarrow |1\rangle.$$

  We see that this is also a familiar operator: $\hat{X}$.
- NOT is the only nontrivial one-bit classical gate. But in quantum mechanics, there are far more possibilities.

- One important example with no classical analogue is the *Hadamard gate*:

$$\hat{U}_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} .$$

- We write these unitaries with a convention similar to that of classical logic gates:

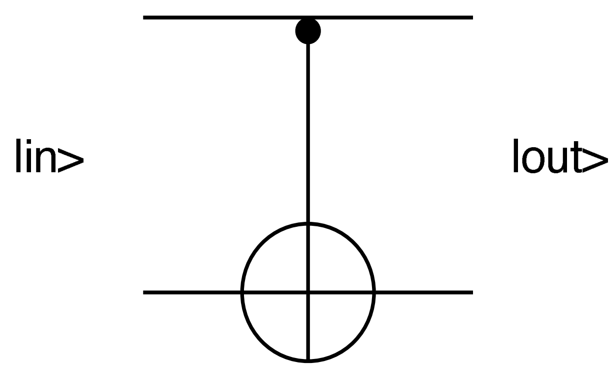


- The *wires* of the circuit diagrams are q-bits, and the *gates* are unitary transformations acting on those qubits. (Such unitaries act on *other* q-bits as the identity.)

- We can also define two-bit quantum gates. One example is the *controlled-not* (CNOT):

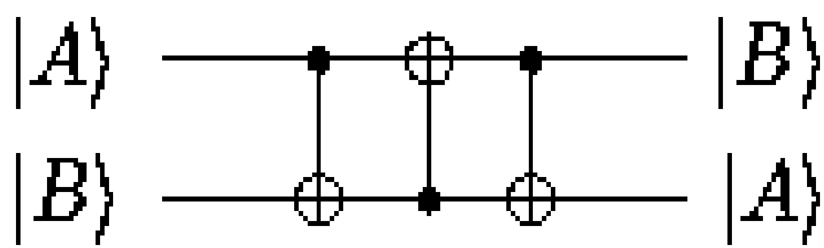
$$\hat{U}_{\mathrm{CNOT}}|00\rangle = |00\rangle, \qquad \hat{U}_{\mathrm{CNOT}}|01\rangle = |01\rangle,$$
$$\hat{U}_{\mathrm{CNOT}}|10\rangle = |11\rangle, \qquad \hat{U}_{\mathrm{CNOT}}|11\rangle = |10\rangle.$$

- Here we write the unitary as a two-bit gate where $|\mathrm{in}\rangle$ and $|\mathrm{out}\rangle$ are now two-bit states:



Quantum circuits

- There are infinitely many possible two-bit gates; but in practice such unitaries are difficult to do. Fortunately, it turns out that just the CNOT (or almost any other two-bit gate), together with one-bit gates, can be used to build up *any* unitary. (We will prove this later in the class!)
- When we combine standard unitary gates, we call the resulting unitary a *quantum circuit*. Here's a simple example that uses three CNOT gates to swap the first and second bits:



- You can check that this this circuit does indeed swap the two q-bits by acting with it on each of the basis states for two q-bits:

$$|00\rangle \to |00\rangle, \qquad |01\rangle \to |10\rangle,$$
$$|10\rangle \to |01\rangle, \qquad |11\rangle \to |11\rangle.$$

  Note that the control and target bits can all be switched, and this will still be a swap gate.

- A quantum circuit for a less trivial unitary will in general be much more complicated. The problem of designing *quantum algorithms* is largely the task of designing such quantum circuits.

- *Next time: some simple examples with light.*