ELEC9705
Lecture 5

Function of an operator

We know how to do basic operations on matrices (sums, products, etc.). How do you calculate a generic function of a matrix, F(A)? For example, $F(A) = e^A$.
$\rightarrow$ use Taylor expansion

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \ldots$$

By analogy:

$$e^A = \sum_{n=0}^{\infty} \frac{A^n}{n!} = \mathbf{1} + A + \frac{A^2}{2} + \frac{A^3}{6} + \ldots$$

This becomes very simple if A is diagonal, since A^n is also diagonal.

$$A = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_N \end{pmatrix} \quad \Rightarrow \quad e^A = \begin{pmatrix} e^{a_1} & & 0 \\ & \ddots & \\ 0 & & e^{a_N} \end{pmatrix}$$

In general, for any function F(A):
if $|\varphi\rangle$ is an eigenvector of A with eigenvalue a
$\Rightarrow |\varphi\rangle$ is also an eigenvector of F(A) with eigenvalue F(a)

Unitary operators

Defined by the property $U^{-1} = U^{\dagger}$.
All Pauli matrices are unitary.
E.g.

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \rightarrow \quad \sigma_y^{\dagger} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_y \sigma_y^{\dagger} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{1} \quad \Rightarrow \quad \sigma_y^{\dagger} = \sigma_y^{-1}$$

Properties of unitary operators:
- Unitary operators conserve the norm of the vector they operate on. Consider:

$$\left|\tilde{\psi}_1\right\rangle = U\left|\psi_1\right\rangle$$

$$\left|\tilde{\psi}_2\right\rangle = U\left|\psi_2\right\rangle$$

$$\left\langle\tilde{\psi}_2 \middle| \tilde{\psi}_1\right\rangle = \left\langle\psi_2 \middle| U^{\dagger}U \middle| \psi_1\right\rangle = \left\langle\psi_2 \middle| \mathbf{1} \middle| \psi_1\right\rangle = \left\langle\psi_2 \middle| \psi_1\right\rangle$$

this means that the norms of the vectors before and after operating with U must be the same

- The eigenvalues of a unitary operator satisfy:

$$\left|\lambda\right| = 1 \quad \Rightarrow \lambda = e^{i\varphi}$$

-The imaginary exponential of a Hermitian operator (meaning $A = A^{\dagger}$) is unitary:

$$T = e^{iA} \rightarrow \quad T^{-1} = e^{-iA} = e^{-iA^{\dagger}} = (e^{iA})^{\dagger} = T^{\dagger}$$

Time-evolution operator

Recall the Schrodinger equation:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}\left|\psi(t)\right\rangle = H\left|\psi(t)\right\rangle$$

It's a set of linear differential equations. Therefore, there must be a linear operator that formally yields the solution:

$$\left|\psi(t)\right\rangle = U(t,t_0)\left|\psi(t_0)\right\rangle$$

with the condition $U(t,t_0) = \mathbf{1}$

Substitute this into the Schrodinger equation:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}U(t,t_0)\left|\psi(t_0)\right\rangle = HU(t,t_0)\left|\psi(t_0)\right\rangle$$

Since $|\psi(t_0)\rangle$ is arbitrary, $U(t,t_0)$ must satisfy:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t}U(t,t_0) = HU(t,t_0)$$

This can be formally integrated to yield:

$$U(t,t_0) = \mathbf{1} - \frac{i}{\hbar}\int_{t_0}^{t} HU(t',t_0)\,\mathrm{d}t' = e^{-iH(t-t_0)/\hbar}$$

The time evolution of a system described by a time-independent Hamiltonian H, starting in an initial state $|\psi(t_0)\rangle$, is:

$$\left|\psi(t)\right\rangle = \exp\left[-iH(t-t_0)/\hbar\right]\left|\psi(t_0)\right\rangle$$

where $U(t,t_0) = \exp\left[-iH(t-t_0)/\hbar\right]$
is the **time evolution operator**

$U(t,t_0)$ is a unitary operator, it conserves the norm of the state. It also time-reversible. Take for simplicity $t_0 = 0$:

$$U(t,0) = U^{-1}(-t,0) \qquad \text{because } U(t,0) = e^{-iHt/\hbar}$$

$$\Rightarrow U(-t,0) = e^{iHt/\hbar}$$

thus, if I know how the system evolved between 0 and t, I can also track its evolution back in time between 0 and $-t$

The time evolution of an isolated quantum system is unitary and time-reversible

Note: if we use as basis of the vector space the eigenstates of the Hamiltonian $\{|\varphi_n\rangle\}$, then H is diagonal, and so is the time-evolution operator $U(t,t_0)$:

$$H = \begin{pmatrix} E_1 & & 0 \\ & \ddots & \\ 0 & & E_N \end{pmatrix}$$

$$\Rightarrow U(t,t_0) = e^{-iH(t-t_0)/\hbar} = \begin{pmatrix} e^{-iE_1(t-t_0)/\hbar} & & 0 \\ & \ddots & \\ 0 & & e^{-iE_N(t-t_0)/\hbar} \end{pmatrix}$$

Therefore the calculation of the time-evolved state

$$|\psi(t)\rangle = U(t,t_0)|\psi(t_0)\rangle$$

reduces to the well-known formula

$$|\psi(t)\rangle = \sum_n c_n(t_0) e^{-iE_n(t-t_0)/\hbar} |\varphi_n\rangle$$

where $|\psi(t_0)\rangle = \sum_n c_n(t_0)|\varphi_n\rangle$

Coupled quantum systems

When looking at single isolated quantum systems (e.g. a spin 1/2) it seemed like we could usually find a classical analog of their quantum behavior.
Things become really striking when considering coupled systems. There we see effects that have no classical analog, like entanglement, which is an important resource for quantum information.

Consider 2 spins. Each one is individually described by 2x2 Pauli matrices. To describe the state of the coupled spins we need a 4-dimensional space (in general, 2^N dimensions for N spins). We can choose as basis of the vector space:

$$|++\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |+-\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |-+\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |--\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

To find an expression for the spin operators, the rule is that the operators for spin 1 should operate in conventional way on 1 while leaving 2 unchanged, and vice versa.
For instance we know that $\sigma_z|+\rangle = |+\rangle$ and $\sigma_z|-\rangle = -|-\rangle$ so now we'll have

$$\sigma_{z1}|++\rangle = |++\rangle; \quad \sigma_{z1}|+-\rangle = |+-\rangle;$$
$$\sigma_{z1}|-+\rangle = -|-+\rangle; \quad \sigma_{z1}|--\rangle = -|--\rangle$$

operates only on spin 1

in matrix form: $$\sigma_{z1} = \begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & -1 & 0\\0 & 0 & 0 & -1\end{pmatrix}$$

and similarly $\sigma_{z2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

For the $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ operator we had $\sigma_x|+\rangle = |-\rangle$

and $\sigma_x|-\rangle = |+\rangle$ (that's why it's sometimes called the "spin flip" operator).

So for 2 spins

$\sigma_{x1}|++\rangle = |-+\rangle; \quad \sigma_{x1}|+-\rangle = |--\rangle;$

$\sigma_{x1}|-+\rangle = |++\rangle; \quad \sigma_{x1}|--\rangle = |+-\rangle$

$\sigma_{x1} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ $\sigma_{x2} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

and similarly

$\sigma_{y1} = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & -i \\ i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix}$ $\sigma_{y2} = \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}$

Information content

The first postulate of QM implies that, given two spins, any state of the form $|\psi\rangle = \alpha|++\rangle + \beta|+-\rangle + \chi|-+\rangle + \delta|--\rangle$ with $|\alpha|^2 + |\beta|^2 + |\chi|^2 + |\delta|^2 = 1$

is a legitimate quantum state of the system.
Therefore, you need 4 (=2^N) complex numbers to fully describe the state of 2 coupled two-level systems.
On the contrary, if you have 2 classical two-level systems (bits), you only need 2 numbers (the two bits)

N fully entangled "quantum bits" (qubits) can contain as much information as 2^N classical bits

To see how important this is, consider the following.
The Universe can be seen as a computer that calculates its own evolution, working at a clock speed ~10^{44} Hz and operating on ~10^{120} bits (these numbers come from constants of nature, mass of the Universe, etc.). That means that the Universe has $2^{10^{120}}$ possible states…

However, notice that $10^{120} \sim 2^{400}$, which is the number of classical bits necessary to describe the state of 400 fully entangled qubits. Thus, 400 fully entangled qubits contain as much information as the entire universe!
However, for this to happen there have to be very delicate non-classical correlations (entanglement), difficult to create and preserve.

Eigenstates of a coupled spin system

Consider the following 2-spin Hamiltonian:

$$H = J\vec{\sigma}_1 \cdot \vec{\sigma}_2 =$$

$$= J\left(\sigma_{x1}\sigma_{x2} + \sigma_{y1}\sigma_{y2} + \sigma_{z1}\sigma_{z2}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

This is called the "Heisenberg exchange Hamiltonian". It represents the energy of two spins that are coupled to each other and nothing else (no magnetic field)

- $J < 0 \Rightarrow$ the spin lower their energy by pointing in the same direction $\rightarrow$ ferromagnetic coupling
- $J > 0$ favors antiparallel spin alignment $\rightarrow$ antiferromagnetic coupling.

The eigenstates of H are:

$$\left|T_+\right\rangle = \left|++\right\rangle$$

$$\left|T_0\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+-\right\rangle + \left|-+\right\rangle\right)$$

$$\left|T_-\right\rangle = \left|--\right\rangle$$

} triplet states

$$\left|S\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+-\right\rangle - \left|-+\right\rangle\right)$$ singlet state

The eigenvalues are:
$E_T = J$ (3-fold degenerate)
$E_S = -3J$
i.e. the singlet-triplet energy splitting is 4J.
Notice that I've used Pauli matrices throughout. If I had accounted for the fact that the actual spins have S=1/2 the splitting would be just *J*.

What is the meaning of these states? As usual, the best way to get a feel for it is to calculate the expectation values of some meaningful quantity.
Consider e.g. the operator representing the sum of the z-projections of the two spins:

$$\sigma_{z,tot} = \sigma_{z1} + \sigma_{z2} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$$

$$\langle T_+ | \sigma_{z,tot} | T_+ \rangle = 2$$

$$\langle T_0 | \sigma_{z,tot} | T_0 \rangle = 0$$

$$\langle T_- | \sigma_{z,tot} | T_- \rangle = -2$$

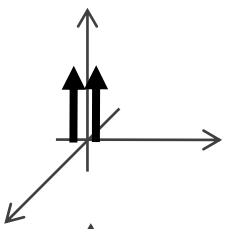
$$\langle S | \sigma_{z,tot} | S \rangle = 0$$

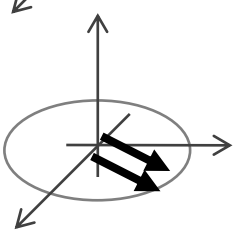
So what's the difference between $|T_0\rangle$ and $|S\rangle$?
Consider the square of the total spin…

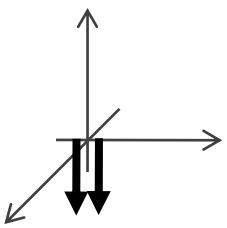
$$\sigma^2 = \left(\sigma_{x1} + \sigma_{x2}\right)^2 + \left(\sigma_{y1} + \sigma_{y2}\right)^2 + \left(\sigma_{z1} + \sigma_{z2}\right)^2 = \begin{pmatrix} 8 & 0 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix}$$

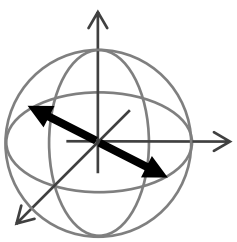
$$\langle T_+ | \sigma^2 | T_+ \rangle = 8$$
$$\langle T_0 | \sigma^2 | T_0 \rangle = 8$$
$$\langle T_- | \sigma^2 | T_- \rangle = 8$$
$$\langle S | \sigma^2 | S \rangle = 0$$

Geometrical interpretation:

$|T_+\rangle$  both spins pointing along +z

$|T_0\rangle$  parallel spins pointing along an undefined direction in the xy-plane

$|T_-\rangle$  both spins pointing along -z

$|S\rangle$  antiparallel spins pointing along an undefined direction in space

Entanglement

Exercise: verify that all the expectation values of the individual spins in the singlet state are zero .
That is:

$$\langle S|\sigma_{x1}|S\rangle = \langle S|\sigma_{x2}|S\rangle = \langle S|\sigma_{y1}|S\rangle = \langle S|\sigma_{y2}|S\rangle =$$
$$= \langle S|\sigma_{z1}|S\rangle = \langle S|\sigma_{z2}|S\rangle = 0$$

This would not be the case in a single spin: at least one of the spin components has to be nonzero!

The singlet state is an "entangled" state that has no classical analog

The individual spins completely lose their identity. The only property of the singlet state is that the spins are antiparallel relative to each other, but you cannot speak about the state of one of the spins alone. The "information" is encoded in the correlation between the spins, not in their individual state .

The existence of nonclassical states like the singlet is the reason why a quantum computer can process much more information that a classical one on the same number of bits.

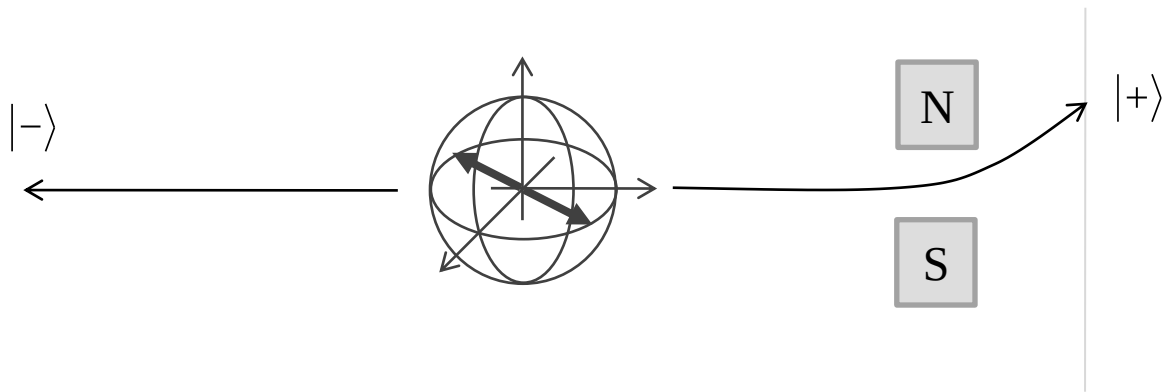
Certain calculations are intractable on a classical computer because their complexity scales exponentially with the number of bits. For example, finding the prime factors of a large number.
On a quantum computer, the existence of extra quantum states can be exploited to reduce the complexity to polynomial, making the problem tractable

Quantum teleportation

Recall the measurement postulate:
"If the measurement of $\mathscr{A}$ at a time *t* has given as a result the value a_n, then, immediately after the measurement, the state of the system is the projection of the initial state $|\psi(t^-)\rangle$ onto the eigenvector $|u_n\rangle$ corresponding to the measured value a_n"

Now assume the 2-spin system is in the state $|S\rangle = (|+-\rangle - |-+\rangle)/\sqrt{2}$ and I want to measure the z-projection of spin 1.
$|+-\rangle$ and $|-+\rangle$ are eigenstates of σ_{z1}, so I will obtain one or the other with probability $1/2 = |\langle +-|S\rangle|^2$ or $|\langle -+|S\rangle|^2$

If I obtain the eigenvalue +1, the state is projected onto $|+-\rangle$, so I know for sure that spin 2 is in the state $|-\rangle$.
This works even if the two spins are far apart!



Logic gates

Time evolution of a quantum state:

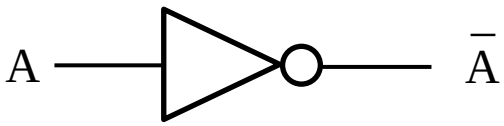
$$|\psi(t)\rangle = U(t,t_0)|\psi(t_0)\rangle$$

Unitary evolution means that no information is lost. Given $|\psi(t)\rangle$ you must be able to reconstruct what was $|\psi(t_0)\rangle = U^{-1}(t,t_0)|\psi(t)\rangle$

This simple statement has a profound consequence on which operations between qubits are allowed!

Classical logic gates:

1-bit gate: NOT



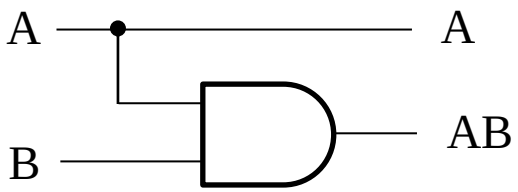
A	$\bar{A}$
0	1
1	0

Knowing the output you can always reconstruct what was the input $\rightarrow$ reversible, no information loss
$\Rightarrow$ has a quantum analog

2-bit gates:

obviously, if you have 2 inputs and 1 output you are losing information. You could e.g. bring forward one of the inputs, in addition to the output

AND

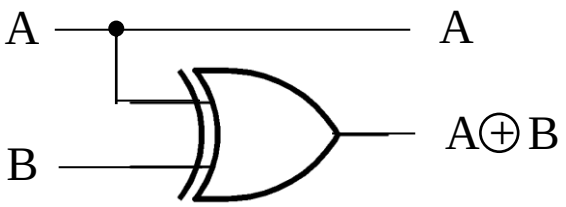


A	B	A	AB
0	0	0	0
0	1	0	0
1	0	1	0
1	1	1	1

there still are 2 different inputs that give the same output

$\Rightarrow$ the AND gate is non-reversible, it can't be made into a quantum gate

XOR



A	B	A	A⊕B
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

now there are no different input having the same output

$\Rightarrow$ the XOR gate is reversible, it can be made into a quantum gate

Quantum versions of the classical logic gates

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

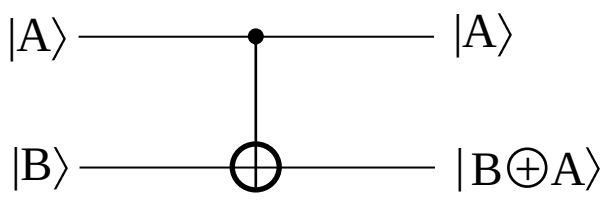
it's the same as the Pauli matrix σ_x, the "spin flip"

Unlike a classical computer, where the bits only take two discrete values, a qubit can be in an arbitrary superposition state. The way the gate operates is still the same. E.g.

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow X|\psi\rangle = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

On a spin, this can be done by pulsed magnetic resonance, with a Rabi rotation of 180 degrees

XOR $\rightarrow$ CNOT ("Controlled NOT")



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

The simple way to describe its action is:

- perform a X (spin flip) operation on $|B\rangle$ if $|A\rangle = |-\rangle$
- do nothing if $|A\rangle = |+\rangle$

Any multiple qubit logic gate can be constructed by combining single-qubit rotations and CNOT operations

…like NAND gates for classical computers