Fundamentals of Quantum Information

Xin Lu/Gentaro Watanabe (gentaro@zju.edu.cn)

Lecture 28

Motivation

- Although modern computers rely on quantum mechanics to operate, the information itself is still encoded classically.
- In recent years, however, research on quantum information technology has revolutionized the way we communicate and process information, though only on a very small scale.
- The new approach is to treat information as a quantum concept and to ask what new insights can be gained by encoding, transmitting, and processing this information in individual quantum systems.

Outline

- Spin, Qubit, and the Bloch Sphere
- Which Way and Quantum Measurement
- Two Qubits, the Bell States, and the EPR Paradox
- Schroedinger's Cat and the Quantum-Classical Boundary

Spin

- As in the context of polarization, we can represent the spin-up and spin-down states by

$$|0\rangle \equiv |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \equiv |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

- An incoming electron can be in a spin state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \qquad a, b \text{ complex.}$$

- The squared magnitudes of the amplitudes give the probabilities of outcomes of measurements, e.g.,

$$P(m_s = 1/2) = |a|^2.$$

Qubit

- The isolated quantum spin is an example of the general class of two-level systems which we call **qubits**, or quantum bits. They are the quantum counterparts of logical bits in classical computers.
- A classical computer operates on strings of zeros and ones, such as 1001001001. Each position in such a string is called a (classical) **bit**, and it contains either a 0 or a 1.
- The abstract bit can be represented by a physical system, such as a capacitor that could be charged (1) or discharged (0), or a magnet whose magnetization could be oriented in two different directions, *up* (0) or *down* (1).

- In quantum mechanics, the two states, which we represent by the symbols $|0\rangle$ and $|1\rangle$, can be superimposed, such that a **qubit** represents

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,.$$

- For example, qubits have been realized by quantum spins in semiconductors, in particular by phosphorus donor electron spins in silicon.
- Researchers have developed a spin qubit fabrication flow using Intel's 300-millimeter process technology that is enabling the production of small spin-qubit arrays in silicon (Intel Labs and QuTech).

From Numbers to Vectors

- In classical computing, we think about numbers. A bit is a binary digit. A string of bits is naturally a binary number.
- Alternatively, we can take the two states of a classical bit to be represented by *two orthogonal unit vectors in a two-dimensional space* (more precisely, *2D Hilbert space*),

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

- The state $|\psi\rangle$ associated with a qubit can be any unit vector in the two-dimensional vector space (**Hilbert space**) spanned by $|0\rangle$ and $|1\rangle$ over the complex numbers.

- The general state of a qubit is

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix},$$

where a and b are two complex numbers constrained only by the requirement that $|\psi\rangle$ should be a unit vector in the complex vector space — i.e., only by the normalization condition:

$$|a|^2 + |b|^2 = 1\,.$$

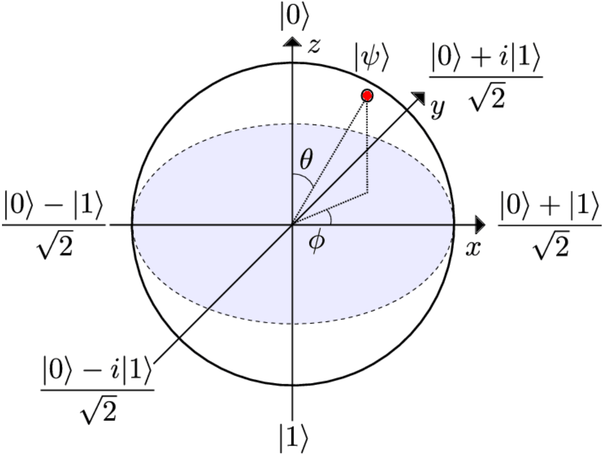
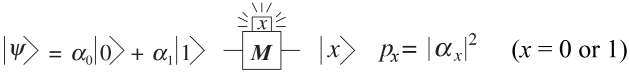


Figure 1: The Bloch sphere representation. The basis states are located at the north and south poles. A spin state can be represented by a point on the Bloch sphere $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$.

Measurement

- To extract information of a qubit in a given state, we make a measurement in the $\{|0\rangle, |1\rangle\}$ basis, which is a certain test on the qubit whose outcome is either 0 or 1.
- The squared magnitudes of the amplitudes give the probabilities of outcomes of measurements.



- More concretely, suppose that we have a qubit in a state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and measure its state in the basis of $\{|0\rangle, |1\rangle\}$. The probability p_x of outcome x $(= 0$ or $1)$ is:

$$p_x = \langle\psi|x\rangle\langle x|\psi\rangle = |\alpha_x|^2.$$

- In fact, the qubit in a quantum superposition of $|0\rangle$ and $|1\rangle$ cannot be viewed as being either in the state $|0\rangle$ or in the state $|1\rangle$ with certain probabilities:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$$\not\Updownarrow$$

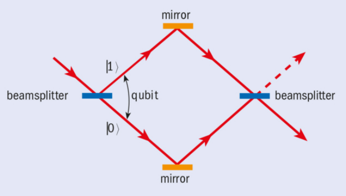
Either in $|0\rangle$ at probability p_0 or $|1\rangle$ at probability p_1.

The latter situation, which is a statistical mixture of $|0\rangle$ and $|1\rangle$, cannot be described by a single wave function. Such a state is called a **mixed state**. On the other hand, the former case described by a single wave function $|\psi\rangle$ is called a **pure state**.

An expanation with a single-photon interferometer

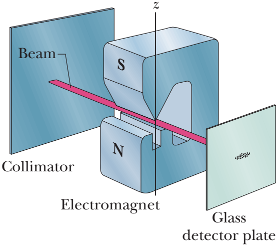
- It can be understood by saying that the particle is in a superposition of the two paths in a single-particle quantum interference: $|0\rangle \equiv |\text{passage along the upper path}\rangle$ and $|1\rangle \equiv |\text{passage along the lower path}\rangle$.

- Measurement is like looking at only one of the ports, say port 1. The probablity to observe the photon is p_1. Once you observe the photon in this port, there must be no photon in the other port, so that the state after the measurement becomes $|1\rangle$ (**reduction of the wave func.**).



An expanation with a Stern-Gerlach apparatus

- In another example, a Stern-Gerlach apparatus with magnetic field in the z axis measures the state of the qubit.



- Quantum measurement is an *irreversible* operation. After the measurement, the qubit is in either $|0\rangle$ or $|1\rangle$. One says that the pre-measurement state *reduces or collapses* to the post-measurement state, as a consequence of the measurement (**Copenhagen interpretation**).

- However, even if S_z has a definite value (i.e., the spin state is $|0\rangle$ or $|1\rangle$), S_x and S_y do not. For example, S_x basis are

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

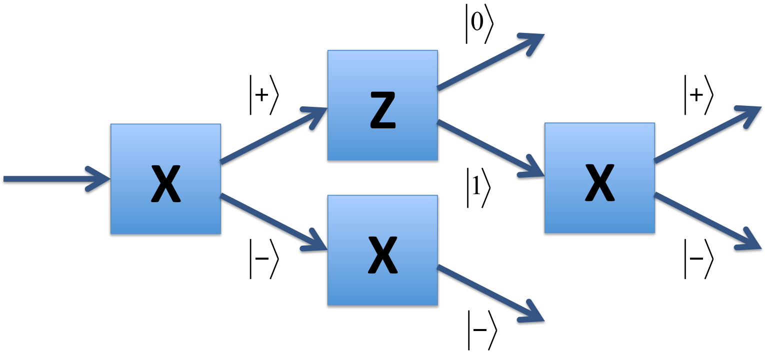
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

  Alternatively, we can write

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle).$$

- So, S_x can still be either $\hbar/2$ or $-\hbar/2$.

- We cannot get around this uncertainty by, say, first measuring S_x and then measuring S_z because the second measurement can change S_x and thus we no longer have a definite value for it.



Appendix: Pauli spin matrices

- x, y, and z-component of spin-1/2 (S_x, S_y, and S_z) are represented by 2×2-matrices called the Pauli spin matrices σ_x, σ_y, and σ_z as

$$S_i = \frac{\hbar}{2}\sigma_i,$$

with

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = -i(|0\rangle\langle 1| - |1\rangle\langle 0|) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = -i(|0\rangle\langle 1| - |1\rangle\langle 0|) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- $\{|0\rangle, |1\rangle\}$ are eigenbasis of σ_z with eigenvalues $\{1, -1\}$: $\{|0\rangle, |1\rangle\}$ are the S_z basis. The state after S_z measurement is either $|0\rangle$ or $|1\rangle$.

- $\{|+\rangle, |-\rangle\}$ are eigenbasis of σ_x with eigenvalues $\{1, -1\}$: $\{|+\rangle, |-\rangle\}$ are the S_x basis. The state after S_x measurement is either $|+\rangle$ or $|-\rangle$.

Two Qubits

- In the case of two bits, the vector space is four-dimensional with an orthonormal basis

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

- The general state $|\Psi\rangle$ that nature allows us to associate with two qubits is any normalized superposition of the four orthogonal basis states,

$$|\Psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

with the complex amplitudes being constrained only by the normalization condition $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

- If the first qubit is in $|0\rangle$, and the second qubit is in $|1\rangle$, then the two-qubit state is $|0\rangle_{\text{1st qubit}} \otimes |1\rangle_{\text{2nd qubit}}$, or $|0\rangle \otimes |1\rangle$, or $|01\rangle$.
- If the first qubit is in $a|0\rangle + b|1\rangle$, and the second qubit is in $c|0\rangle + d|1\rangle$, then the two-qubit state is

$$\begin{aligned} &(a|0\rangle + b|1\rangle)_{\text{1st qubit}} \otimes (c|0\rangle + d|1\rangle)_{\text{2nd qubit}} \\ = \; & ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned}$$

- In this case, even though we put the two qubits togather, the information they encode is still *separable* between the two qubits. If we operate on the first qubit only, the second remains unchanged.

Bell States

- There is another set of states, exemplified by the famous Bell states. One of the four Bell states is

$$|\Psi_{+}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right).$$

- In the state, particle 1 can be in state $|0\rangle$ and particle 2 in state $|1\rangle$, or vice versa, but there is no way of knowing which particle is in which state. All that is defined is the fact that the two qubits are different.

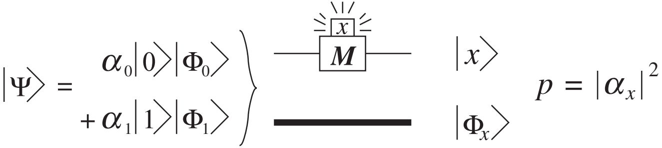
- The key point is that the single-particle states are **entangled** in such superpositions. This means that the two-particle Bell state cannot be written as the tensor product of single-particle states.
- This means that all of the information is distributed among two qubits, and that none of the individual systems carries any information. This is the essence of **entanglement** and is one of the novel and counterintuitive features of quantum mechanics.

Measuring Entangled Particles

- We can measure the first qubit of the state:

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right),$$

according to the following measurement rule



- More explicitly, suppose that two qubits are in the state of $|\psi\rangle = \alpha_0|0\rangle|\Phi_0\rangle + \alpha_2|1\rangle|\Phi_1\rangle$ and we measure the state of the first qubit in the basis of $\{|0\rangle, |1\rangle\}$. The probability p_x of outcome x $(= 0 \text{ or } 1)$ is:

$$
\begin{aligned}
p_x =& \langle\psi| \left(|x\rangle\langle x| \otimes I_2\right) |\psi\rangle \\
=& \left(\alpha_0^*\langle 0|\langle\Phi_0| + \alpha_2^*\langle 1|\langle\Phi_1|\right) \left(|x\rangle\langle x| \otimes I_2\right) \\
& \left(\alpha_0|0\rangle|\Phi_0\rangle + \alpha_2|1\rangle|\Phi_1\rangle\right) \\
=& |\alpha_x|^2.
\end{aligned}
$$

Here, I_2 is the identity in the Hilbert space of the second qubit.

EPR Paradox

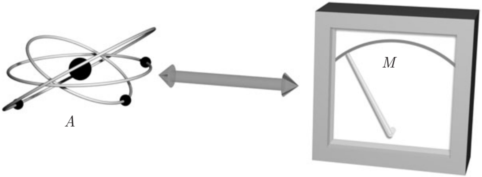
- Entanglement is closely linked to the issue of non-locality in quantum theory.
- In particular, if the two particles in an entangled state are widely separated, then a measurement on one will immediately influence the quantum state of the other one. It seems as if the particles are communicating faster than the speed of light.
- Because of this, Einstein and coworkers resisted the idea that quantum mechanics could provide a complete description of reality [Einstein, Podolsky, and Rosen, *Phys. Rev.* **47**, 777 (1935)].

- In Bohm's version of the EPR paradox, two particles are in the Bell state

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right).$$

  Today, experiments can show that after they are sent far apart, their properties remain entangled.
- Measurement of particle 1 affects particle 2 instantaneously. But special relativity is not violated because no information is exchanged. (Do you see why?)
- **There is still a speed limit for information transfer.**

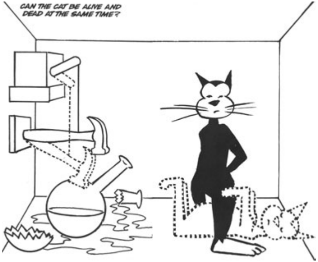
- Unlike in classical computation, entanglement is a fundamentally new resource crucial in quantum error correction and quantum parallelism.
- Even though the quantum mechanical theory can be made self-consistent, quantum entanglement simply teaches us just how strange the quantum world really is. But what about the entanglement between microscopic and macroscopic systems?



The Schroedinger Cat Paradox

- Quantum measurement generally encounter entanglement between microscopic and macroscopic systems, such as an atom and a Stern-Gerlach apparatus.
  Namely, by making correlation between the microscopic quantum system which we want to measure and the probe in the macroscopic apparatus, relevant information of the former is transferred to the latter.
  Finally, the state of the microscopic quantum system is reflected to the meter of the apparatus, so that the system is measured by the readout of the meter.

- Schroedinger (1935) dramatize it by introducing a fictitious cat, whose *living* and *dead* states are entangled to the atomic states in a radiative decay.



There is a radioactive atom A which is in a superposition of undecayed state $|0_A\rangle$ and decayed state $|1_A\rangle$ with 50 : 50 probability.

The radiation of the atom is monitored by a detector, which is connected to the hammer that shatters the flask of poison if the ratiation is detected. Thus the undecayed state $|0_A\rangle$ of the atom leads to the living state $|0_C\rangle$ of the cat C while the decayed state $|1_A\rangle$ leads to the dead state $|0_C\rangle$:

$$|\psi_{A+C}\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle\,|0_C\rangle + |1_A\rangle\,|1_C\rangle).$$

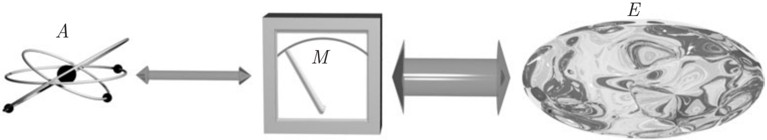
- If we open the box and see a living cat ($|0_C\rangle$), the atom is in the corresponding $|0_A\rangle$ state. If we see a dead cat ($|1_C\rangle$), the atom is in the $|1_A\rangle$ state.
- Apparently, this is the same as the EPR paradox. But such a state can also be expressed as

$$|\psi_{A+C}\rangle = \frac{1}{\sqrt{2}}\left[\frac{|0_A\rangle + |1_A\rangle}{\sqrt{2}}\frac{|0_C\rangle + |1_C\rangle}{\sqrt{2}} + \frac{|0_A\rangle - |1_A\rangle}{\sqrt{2}}\frac{|0_C\rangle - |1_C\rangle}{\sqrt{2}}\right].$$

- Is it possible that the atom is in a state $(|0_A\rangle + |1_A\rangle)/\sqrt{2}$, while the cat is apparently half living and half dead $(|0_C\rangle + |1_C\rangle)/\sqrt{2}$? What does that mean?

- It turns out when we come to the macroscopic world, the cat state is really couple to a large environment E (the whole cat itself).
- The whole system (if we assume the environment is initially in a pure state) is

$$\left|\psi_{A+C+E}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_A\right\rangle\left|0_C\right\rangle\left|\zeta_E^0\right\rangle + \left|1_A\right\rangle\left|1_C\right\rangle\left|\zeta_E^1\right\rangle\right).$$



- In other words, we can say that the coupling to the environment functions as a measurement, which leaks the information of the living or dead state, even though our human observers are not looking.
- Therefore, the presence of a large object (the real cat) at different macroscopic states (e.g., positions of the cat) influences the microscopic state, so the coherence between the living and dead states associated to, e.g., different positions vanishes (hence the name **decoherence**).
- As a result, the environmental measurement prevents interference effects from building up between the living and dead states. Very quickly, *the cat is either dead or alive and not in a superposition of the two states*.

Summary

- Quantum physics is most strange in the following aspects:
  - Superposition of wave functions in Hilbert space
  - Which-way measurement and quantum interference
  - EPR paradox and quantum entanglement
  - Schroedinger's cat and the quantum-classical boundary
  - Identical particles and quantum condensation
- Today, we are trying our best to tame the quantum strangeness to process information.