Spooky action at a distance?

Quantum entanglement, statistical physics, and the arrow of time

Laura Cui

November 2021

HMMT Education

Quantum computing

$\underbrace{\textbf{Quantum}}_{\text{Physics}}$ **computing**

$$\underbrace{\textbf{Quantum}}_{\text{Physics}}\ \overbrace{\textbf{computing}}^{\text{Computer science}}$$

Introduction (cont.)

- **Quantum computing** is the application of quantum mechanical phenomena to perform computations
- Information or data can be stored as the state of a physical system
- The operation of a quantum computer is tied to the underlying physics

Why quantum computing?

- Certain quantum effects are difficult to simulate classically
- Quantum computers are believed to be capable of completing some tasks much faster than classical computers
    - Example: factoring large integers (Shor's algorithm)
- Finding connections can improve understanding of fundamental questions

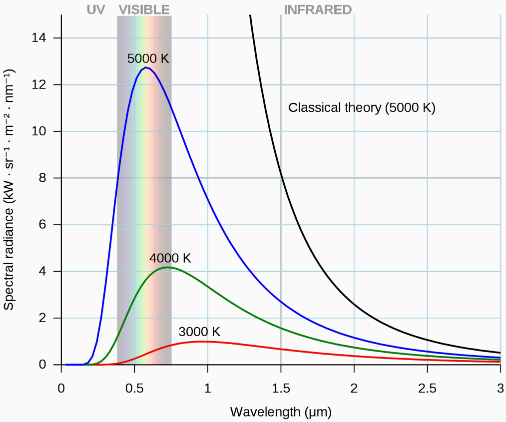
Quantum mechanics

The history of modern physics

- By early 1900's most of physics was thought to be solved
- Newtonian mechanics and Maxwell's equations seemed to accurately describe matter and light
- In 1900, Lord Kelvin proclaimed "there is nothing new to be discovered in physics. All that remains is more and more precise measurement."

Inconsistencies c. 1900

- Ultraviolet catastrophe: infinite amount of energy predicted in thermal radiation since classical distribution $B \propto \frac{1}{\lambda^4}$



Inconsistencies c. 1900 (cont.)

- Photoelectric effect: electrons are released when shining light onto metal
- Kinetic energies depend only on the wavelength of light and not the intensity
- In 1900 Planck determined the correct distribution for thermal radiation

$$B \propto \frac{\nu^3}{e^{h\nu/k_B T} - 1}, \quad \nu = c/\lambda$$

- In 1905 Einstein proposed quanta with $E = h\nu$ to explain photoelectric effect

Postulates of quantum mechanics

1. An isolated physical system is associated with a **state space** complex vector space with an inner product. At any point in time, the system is described by its **state vector**, a vector in this space which represents the wavefunction.

Postulates of quantum mechanics (cont.)

1. An **isolated** physical system is associated with a **state space** complex vector space with an inner product. At any point in time, the system is described by its **state vector**, a vector in this space, a vector in this space which represents the wavefunction.

Postulates of quantum mechanics (cont.)

1. An isolated physical system is associated with a **state space** **complex vector space** with an **inner product**. At any point in time, the system is described by its **state vector**, a vector in this space, a vector in this space which represents the wavefunction.

Postulates of quantum mechanics (cont.)

- Analogous to Euclidean vector spaces, e.g. $\mathbb{R}^2$
- A set of vectors S **spans** a vector space V if V is equal to the set of all **linear combinations** of elements of S
  - Does $\{\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]\}$ span $\mathbb{R}^2$? What about $\{\left[\begin{smallmatrix}2\\-1\end{smallmatrix}\right], \left[\begin{smallmatrix}-4\\2\end{smallmatrix}\right]\}$?
- A **basis** B of a vector space V is a minimum spanning set of V
  - Notice $|B| = \dim V$

Postulates of quantum mechanics (cont.)

- The **inner product** of two vectors $\vec{a}$ and $\vec{b}$ defines ”how much of $\vec{a}$ is in $\vec{b}$”
  - The inner product for $\mathbb{R}^2$ is just the dot product $\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2$
- For any vector $\vec{a}$, $\left|\vec{a}\right| = \sqrt{\vec{a} \cdot \vec{a}}$
- Two vectors $\vec{a}$ and $\vec{b}$ are **orthogonal** if $\vec{a} \cdot \vec{b} = 0$
- If two vectors $\vec{a}, \vec{a}' \in \mathbb{R}^2$ are orthogonal, then any vector $\vec{b} \in \mathbb{R}^2$ can be written as $\vec{b} = \frac{\vec{b} \cdot \vec{a}}{\left|\vec{a}\right|}\vec{a} + \frac{\vec{b} \cdot \vec{a}'}{\left|\vec{a}'\right|}\vec{a}'$
  - Example: the vector $\left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right]$ can be written as $3\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right]$

Postulates of quantum mechanics (cont.)

- In quantum mechanics the coefficients can be *complex* numbers
- Quantum state vectors often written as **kets**, i.e. $|\psi\rangle$
- If a two-level system is spanned by a set $\{|\psi_1\rangle, |\psi_2\rangle$, then any state $|\psi\rangle$ can be written as a sum $\{c_1 |\psi_1\rangle + c_2 |\psi_2\rangle$
- Example: in Schrödinger's thought experiment, a cat is placed in a box, and nuclear radiation is released with some probability
  - The cat's state is given by $c_1 |\text{dead}\rangle + c_2 |\text{alive}\rangle$ for some complex c_1, c_2

Postulates of quantum mechanics (cont.)

- The inner product of two states $|a\rangle = a_1 |\psi_1\rangle + a_2 |\psi_2\rangle$ and $|b\rangle = b_1 |\psi_1\rangle + b_2 |\psi_2\rangle$ is given by $\langle a|b\rangle = a_1^* b_1 + a_2^* b_2$
- Notice $\langle a|b\rangle = \langle b|a\rangle^*$ for any two states $|a\rangle$, $|b\rangle$
- $\langle a|a\rangle = |a_1|^2 + |a_2|^2$ is always real and non-negative
    - Assumed to be equal to 1 so that states are normalized

Postulates of quantum mechanics (cont.)

2. The evolution of a closed quantum system is described by a unitary transformation.

Postulates of quantum mechanics (cont.)

2. The evolution of a **closed** quantum system is described by a unitary transformation.

2. The evolution of a closed quantum system is described by a **unitary transformation**.

Postulates of quantum mechanics (cont.)

- Given the state of the system $|\psi\rangle$ at some time t_0, the state of the system at any other time t can be given as $|\psi'\rangle = U(t)\,|\psi\rangle$, such that $\langle\psi|\psi\rangle = \langle\psi'|\psi'\rangle$
- U must be a **linear operator**, so for any $|\psi\rangle = c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle$, $U\,|\psi\rangle = c_1 U\,|\psi_1\rangle + c_2 U\,|\psi_2\rangle$
- Is $U = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ a valid transformation? What about $U = \left[\begin{smallmatrix} i & 0 \\ 1 & 0 \end{smallmatrix}\right]$?
- Note that U can represent the natural evolution of the system or manipulations in a quantum circuit

Postulates of quantum mechanics (cont.)

3. Quantum measurements project the system onto an orthonormal basis of possible outcomes.

Postulates of quantum mechanics (cont.)

3. Quantum measurements project the system onto an **orthonormal basis** of possible outcomes.

Postulates of quantum mechanics (cont.)

- A system whose state is given by $|\psi\rangle = c_1 |\psi_1\rangle + c_2 |\psi_2\rangle$ will be observed in the $|\psi_1\rangle$ state with probability $|\langle\psi|\psi_1\rangle|^2 = |c_1|^2$, and in the $|\psi_2\rangle$ state with probability $|\langle\psi|\psi_2\rangle|^2 = |c_2|^2$
    - Recall by convention we set $|c_1|^2 + |c_2|^2 = 1$
    - Can't directly measure c_1 and c_2
- Example: if Schrödinger's cat is in the state $|\psi_{\text{cat}}\rangle = \frac{1}{2} |\text{dead}\rangle + \frac{\sqrt{3}}{2} |\text{alive}\rangle$, there is a $\frac{1}{4}$ chance of observing it dead and $3/4$ chance of observing it alive when we open the box

Mixed states

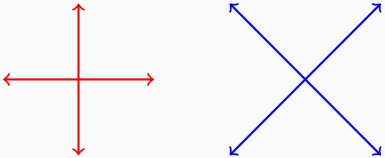
- In addition to pure quantum states, we can also consider *classical* probabilistic ensembles of different states or **mixed states**
- Example: a coin toss lands on either heads or tails with probability $1/2$
- Behave differently from superpositions when measured in different bases

Photon polarization

- Polarizing filters project photons along either the X or Y axes, allowing only photons along the X axis to pass through
- If the initial beam is unpolarized, a photon's initial state can be represented as $\frac{1}{\sqrt{2}}\left|x\right\rangle + \frac{1}{\sqrt{2}}\left|y\right\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1/\sqrt{2} \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$
- Photons are projected onto the state $\left|x\right\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and pass through with probability $1/2$

Photon polarization (cont.)

- If the polarized beam is passed through another filter rotated by 45°, photons are projected onto $|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$ and pass through with probability $1/2$
- If the outgoing beam is passed through yet another filter rotated by 90°, photons are projected onto $|y\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and pass through with probability $1/2$
- The final output beam is orthogonal to the original polarized beam!



$\left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}$ $\left\{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}\right\}$

Photon polarization (cont.)

- Note if a beam polarized in the $|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$ direction is passed through another filter offset by 45°, all of the photons will pass through
- A mixed state can be prepared by combining a beam passed through the first filter with a beam passed through a filter rotated by 90°
  - Any given photon is either in the state $|x\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ or $|y\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ with probability $1/2$
  - If this beam is passed through a filter offset by 45°, only $1/2$ of the photons will pass through!

Quantum bits

- Classical bits can take on the values 0 or 1
- Quantum bits or **qubits** can be in any superposition of $|0\rangle$ and $|1\rangle$
- A general qubit state is given by $a|0\rangle + b|1\rangle$, where a and b are complex
    - Suggests a single qubit can store more information than a classical bit

Quantum entanglement

Composite systems

- Often interested in systems with multiple components
- **Composite systems** are associated with a vector space represented by the tensor product of its component vector spaces
  - If we have two classical coins, the outcome is one of $\{\mathrm{HH}, \mathrm{HT}, \mathrm{TH}, \mathrm{TT}\}$
  - If we have two cats in boxes Mittens and Nora, the state of the system is spanned by the basis $\{|\text{alive}\rangle_M \otimes |\text{alive}\rangle_N, |\text{alive}\rangle_M \otimes |\text{dead}\rangle_N, |\text{dead}\rangle_M \otimes |\text{alive}\rangle_N, |\text{dead}\rangle_M \otimes |\text{dead}\rangle_N\}$
  - The state of a two-qubit system AB is spanned by the basis $\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}$, or $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

Entanglement

- The outcomes of two coin flips is always independent, i.e. landing on heads for one doesn't affect the probability of landing on heads for the other
- Two components of a composite quantum system are **entangled** if the distribution of their measurement outcomes is *not* independent
- Example: is the state $|\psi\rangle_{MN} = |\text{alive}\rangle_M \otimes |\text{alive}\rangle_N$ entangled?
  - No, no matter which cat we check first, we always find that both are alive

Entanglement (cont.).

Which of the following qubit states are entangled?

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{8}}|00\rangle + \frac{\sqrt{3}}{\sqrt{8}}|01\rangle + \frac{1}{\sqrt{8}}|10\rangle + \frac{\sqrt{3}}{\sqrt{8}}|11\rangle$$

- Not entangled, regardless of the outcome of A we always have $1/4$ chance of measuring B in the $|0\rangle$ state and $3/4$ chance of the $|1\rangle$ state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- Entangled, if we measure A in the $|0\rangle$ state we will always measure B in the $|0\rangle$ state, and vice versa
- Example of a **maximally entangled state**, also one of the **Bell states**

Entanglement (cont.)

- Equivalent definition: a two-system state is entangled if the composite state cannot be factored
  - $\frac{1}{\sqrt{8}}\left|00\right\rangle + \frac{\sqrt{3}}{\sqrt{8}}\left|01\right\rangle + \frac{1}{\sqrt{8}}\left|10\right\rangle + \frac{\sqrt{3}}{\sqrt{8}}\left|11\right\rangle = \left(\frac{1}{\sqrt{2}}\left|0\right\rangle_A + \frac{1}{\sqrt{2}}\left|1\right\rangle_A\right)\left(\frac{1}{2}\left|0\right\rangle_B + \frac{\sqrt{3}}{2}\left|1\right\rangle_B\right)$
- Entanglement is generated by interactions between the two subsystems
- States can be prepared using an **entangling gate** such as CNOT (”controlled NOT”), which flips the second qubit if the first qubit is 1

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{CNOT}\frac{1}{\sqrt{2}}(\left|0\right\rangle_A + \left|1\right\rangle_A)\left|0\right\rangle_B = \frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle$$

Entanglement (cont.)

- A pair of qubits which are maximally entangled is also known as an **EPR pair** (short for Einstein–Podolsky–Rosen)
- Bell states $\{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$ form alternative basis for two-qubit system
- Is it possible for Alice to send Bob two bits of classical information by sending only one qubit?
    - Yes, if Alice and Bob share an EPR pair beforehand
    - Known as **superdense coding**

Quantum game theory

- Quantum game theory allows for strategies which take advantage of effects such as quantum operations or entanglement
- Players may improve their chances of winning without directly communicating if they share entangled qubits

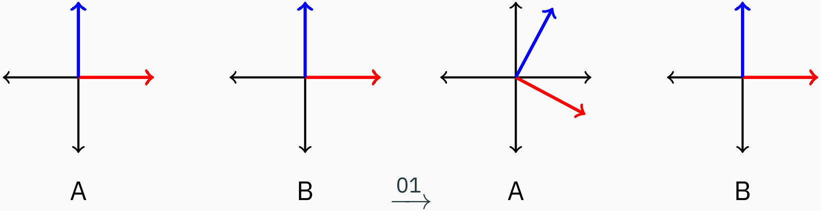
Quantum game theory (cont.)

- Alice and Bob play a game where they each receive a challenge bit and must send another bit in response; they win if the challenge string was 00 and the sum of the response bits is odd, or if the challenge string was anything else and the sum of the response bits is even
- What is the best probability of winning they can get playing classically?
- If Alice and Bob are allowed to share an EPR pair, what is their maximum probability of winning?

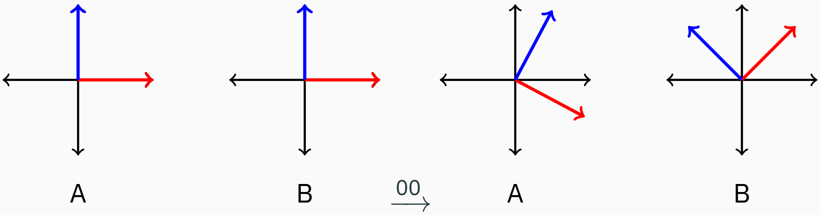
Quantum game theory (cont.)

- Solution: Alice agrees to rotate her state by -22.5° if she receives a 0 and 22.5° if she receives a 1
- Bob rotates his state by 45° if he receives a 0 and 0° if he receives a 1
- States are offset by 67.5° if the challenge string is 00 and 22.5° otherwise
  - They win with probability $\cos(22.5^\circ)^2 \approx 0.85$ no matter the challenge string

Quantum game theory (cont.)



Quantum game theory (cont.)



Information theory

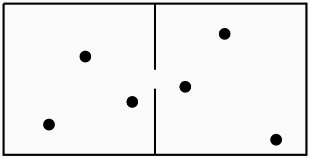
What is information?

- Roughly “how much we know about the state of something”
- Classical information theory typically focuses on digital information
- Practical applications in file compression schemes

History of thermodynamics

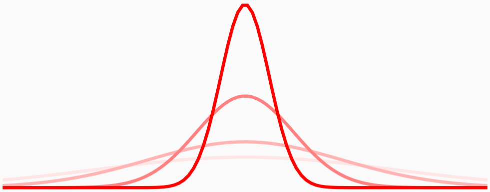
- Classical thermodynamics focuses on describing systems near equilibrium
- Inspired by invention of technologies such as steam engine in early 1700s
- Relates changes in macroscopic properties such as temperature, pressure, volume, energy transfer as work or heat
- **Entropy** comes from definition of energy lost as heat $\Delta Q = T\Delta S$

- Developed after theory of atoms and molecules in late 1800s–early 1900s
- Observable **macrostate** includes many **microstates** or exact configurations
  - Example: equal pressure in two parts of a sealed chamber
- Boltzmann formula for a macrostate with Ω microstates gives $S = k_B \log \Omega$



Statistical mechanics (cont.)

- Emergent behavior can be understood through **central limit theorem**
- Distribution of average particle energy or other variables becomes infinitely narrow as size of the system goes to infinity



Shannon entropy

- First proposed by Shannon in 1948 to formalize information
- For discrete random variable X, its Shannon entropy is given by

$$H(X) = -\sum p(x_i) \log p(x_i)$$

- Name "entropy" suggested by Von Neumann due to similarity to physics
- Quantifies degree of uncertainty regarding the outcome

Shannon entropy (cont.)

- What is the entropy of a fair coin?
  - $-\sum \frac{1}{2} \log(1/2) = -\log(1/2) = 1$
- What about a coin which only has a $1/1024$ chance of heads?
  - $-(1 - \frac{1}{1024}) \log_2(1 - 1/1024) - \frac{1}{1024} \log_2(1/1024) \approx 0.01$
- What is the maximum allowed entropy of a discrete random variable which can take on n different outcomes?
  - $-\sum \frac{1}{n} \log(1/n) = -\log n$

Shannon source coding theorem

- A string of N i.i.d.[1] variables with entropy H can be compressed into more than NH bits such that probability of information loss is asymptotically zero
- If a string of N i.i.d. variables is compressed into less than NH bits then the asymptotic rate of information loss is constant and nonzero

[1] independent and identically distributed

Shannon source coding theorem (cont.)

- Intuition: the frequency of English letters in a very long passage should be similar to their overall frequency in the language
- In the limit as $N \to \infty$, the number of times that each letter appears is equal to its expected value

$$NH = -N \sum p_i \log p_i = -\sum \mathbb{E}[N_i] \log p_i = -\log \prod p_i^{\mathbb{E}[N_i]}$$

The arrow of time

Reversibility

- The microscopic laws of physics are (mostly) invariant under time reversal
- Examples and/or exceptions
  - Parabolic motion of object thrown near Earth’s surface
  - Unitary (and reversible) evolution in quantum mechanics
- Intuitively, time appears to run in a particular direction

Reversibility (cont.)

Second law of thermodynamics

- States that the entropy of a closed system can never decrease
- A process is reversible if there is no change in entropy
- Also implies that entropy must be maximized at equilibrium
- **Thermalization** is process in which system moves towards equilibrium

Information scrambling

- **Entanglement entropy** extends Shannon and Gibbs entropy to measurement of quantum systems
- Quantum interactions cause parts of system to become entangled which prevents information from being extracted, hence **scrambling** the system
- Active area of research with applications to quantum state tomography, condensed matter theory, and black hole physics

Conclusion

Quantum computing technology

- Noisy intermediate-scale quantum (NISQ) devices may be available soon
- Google quantum supremacy announcement in October 2019
- Quantum cryptography and secure communication applications
  - Quantum key distribution implementations have been demonstrated on distances of over 300 miles

Outlook

- Exciting connections between historically disjoint fields
- New tools and techniques to describe physical systems
    - Recent progress in understanding emergent behavior of large quantum systems
- Perspectives from physics also contribute to advances in computing