LABORATOIRE
D'INFORMATIQUE
& DES SYSTÈMES

CANA seminar:

Introduction to quantum information theory

Nasra DAHER AHMED

Outline

1. From classical to quantum information theory
2. Mathematical formalism of quantum mechanics
3. Entanglement and the CHSH game
4. No-go theorems (Bell’s, no-cloning)
5. Quantum teleportation

1. From classical to quantum information theory

- Classical information theory: how to store/transmit *classical* information.
- Formalized by Claude Shannon in his seminal article of 1948, answered important questions:

1. How can we quantify information?
2. What is the optimal data compression rate? (Noiseless coding)
3. What is the optimal rate of transmission over a noisy channel? (Noisy-channel coding)

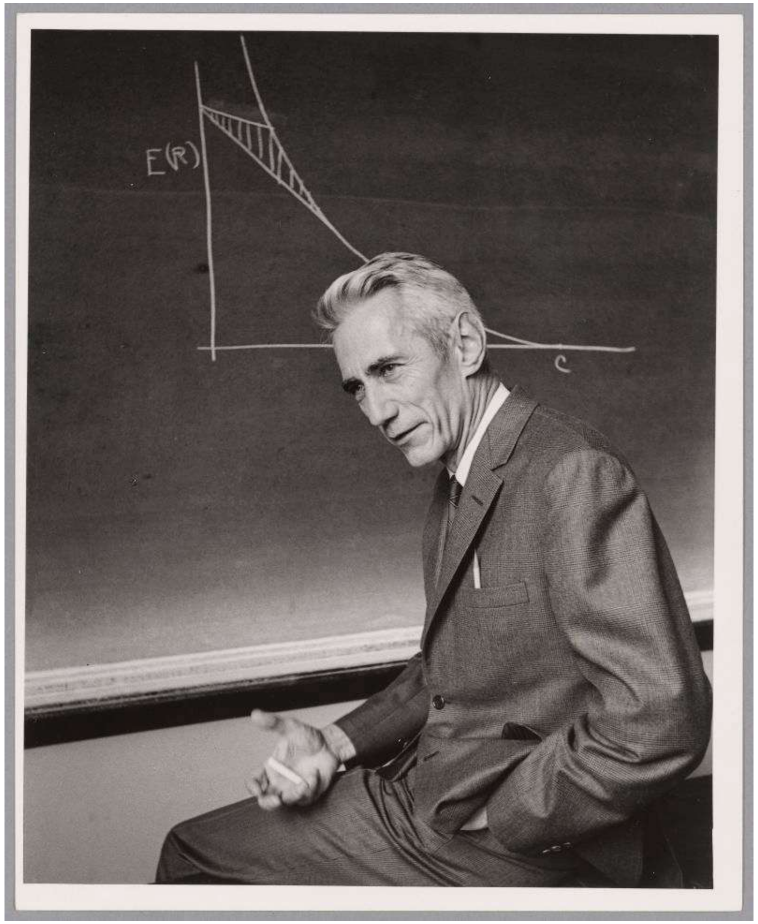


Image source: MIT museum

1. From classical to quantum information theory

- Development of quantum theory since the 20s, a focus on foundations (e.g. **Bell's theorem** in 1964).

→ Quantum information theory: how we can store/transmit *quantum* information.

- Some breakthroughs in quantum information theory:

1. Holevo's bound on the accessible information about a quantum state (1973)

2. **No-cloning theorem** (1970, 1982)

1. From classical to quantum information theory

- Some breakthroughs in quantum information theory (cont.):

3. BB84: first quantum key distribution protocol (1984)

4. **Quantum teleportation (1993)**

5. Quantum Shannon theory: Schumacher's quantum noiseless coding (1995)

Mathematical formalism of quantum mechanics

1. State (pure)

The state of a quantum system is described by a unit vector $|\psi\rangle$ *in a complex Hilbert space* $\mathcal{H}$ (state space).

Example: $\mathcal{H} = \mathbb{C}^2$

- "kets" $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ as column vectors (computational basis)
- "bras" $\langle 0| = |0\rangle^\dagger = (|0\rangle^*)^T = (1 \quad 0)$ and $\langle 1| = (0 \quad 1)$ as row vectors

Mathematical formalism of quantum mechanics

1. **State (pure)**

Example: $\mathcal{H} = \mathbb{C}^2$

- General state in $\mathbb{C}^2$ is a superposition/a qubit:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ = $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ with $\alpha, \beta \in \mathbb{C}$

1. Normalized: $\langle\psi|\psi\rangle = (|\psi\rangle^*)^T|\psi\rangle = (\alpha^* \quad \beta^*)\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 + |\beta|^2 = 1$

2. Unique up to a unit global factor: $\gamma|\psi\rangle$ = $|\psi\rangle, \gamma \in \mathbb{C}$ s.t. $|\gamma| = 1$

Mathematical formalism of quantum mechanics

2. Unitary evolution:

The evolution of $|\psi\rangle$ *is described by a unitary operation* $|\psi'\rangle = U|\psi\rangle$ *(*$UU^\dagger = \mathbb{I}$*).*

Why unitary?

1. Reversible: $|\psi\rangle = U^\dagger|\psi'\rangle$.
2. Preserves the norm: $\langle\psi'| = \langle\psi|U^\dagger, \langle\psi'|\psi'\rangle = \left\langle\psi\middle|U^\dagger U\middle|\psi\right\rangle = \langle\psi|\psi\rangle = 1.$

Mathematical formalism of quantum mechanics

2. Unitary evolution:

The evolution of $|\psi\rangle$ *is described by a unitary operation* $|\psi'\rangle = U|\psi\rangle$ $(UU^\dagger = \mathbb{I})$.

Example: $\mathcal{H} = \mathbb{C}^2$

1. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ s.t. $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$ (X-Pauli operator).

2. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ s.t. $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
   and $H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (Hadamard operator).

Mathematical formalism of quantum mechanics

3. Measurement:

Given a system in a state $|\psi\rangle$, any observable (physical property) of the system is described by a Hermitian operator A ($A^\dagger = A$):

1. *The observable takes values in the set of eigenvalues of A (which are all real).*

2. *The probability of measuring an eigenvalue λ_k is given by $p_{\lambda_k} = |\langle\psi_k|\psi\rangle|^2$.*

3. *The state of the system after the measurement is $(\frac{\langle\psi_k|\psi\rangle}{|\langle\psi_k|\psi\rangle|})|\psi_k\rangle$.*

Mathematical formalism of quantum mechanics

3. Measurement:

Example: $\mathcal{H} = \mathbb{C}^2$

1. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ s.t. $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$ (Z-Pauli operator).

- Eigenvalues $+\mathbf{1}$ for $|0\rangle$ and $-\mathbf{1}$ for $|1\rangle$.

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $p_{+1} = |\alpha|^2$ and $p_{-1} = |\beta|^2$.

Mathematical formalism of quantum mechanics

3. Measurement:

Example: $\mathcal{H} = \mathbb{C}^2$

2. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ s.t. $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$ (X-Pauli operator).

- $X|+\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) = |+\rangle$ and $X|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = -|-\rangle$
  so eigenvalues $+\mathbf{1}$ for $|+\rangle$ and $-\mathbf{1}$ for $|-\rangle$.

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$, $p_{+1} = |\frac{\alpha+\beta}{\sqrt{2}}|^2$ and $p_{-1} = |\frac{\alpha-\beta}{\sqrt{2}}|^2$.

Mathematical formalism of quantum mechanics

4. Composite systems:

The state space of a composite system $S = S_1 \ldots S_N$ is $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{\mathrm{N}}$.

Example: $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, *computational basis.*

$$|00\rangle = |0\rangle \otimes |0\rangle = \binom{1}{0} \otimes \binom{1}{0} = \begin{pmatrix} 1 \binom{1}{0} \\ 0 \binom{1}{0} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \text{ and } |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Mathematical formalism of quantum mechanics

4. Composite systems:

Example: $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, Bell states.

$$|\phi^+\rangle_{S_1S_2} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\phi^-\rangle_{S_1S_2} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^+\rangle_{S_1S_2} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\psi^-\rangle_{S_1S_2} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Entanglement and the CHSH game

- Definition: A composite pure state $|\psi\rangle_{S_1\dots S_N}$ is *entangled* iff it cannot be written as a product $|\psi_1\rangle_{S_1} \otimes \cdots \otimes |\psi_N\rangle_{S_N}$, otherwise it is *separable*.
  Example: $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$

$$|\psi\rangle_{S_1S_2} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |++\rangle$$

v.s.

$$|\phi^+\rangle_{S_1S_2} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Entanglement and the CHSH game

- Intuitively: The parts of the state are *correlated.*

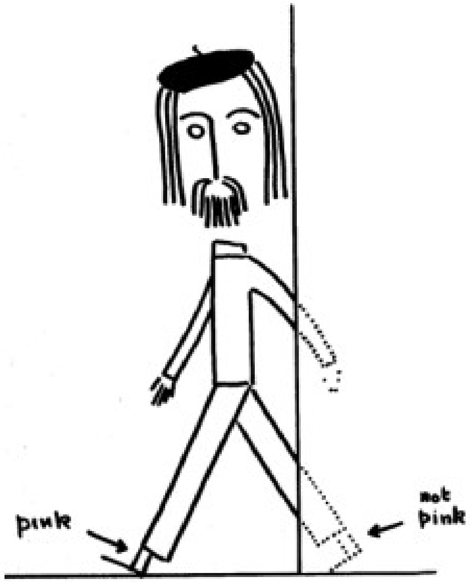
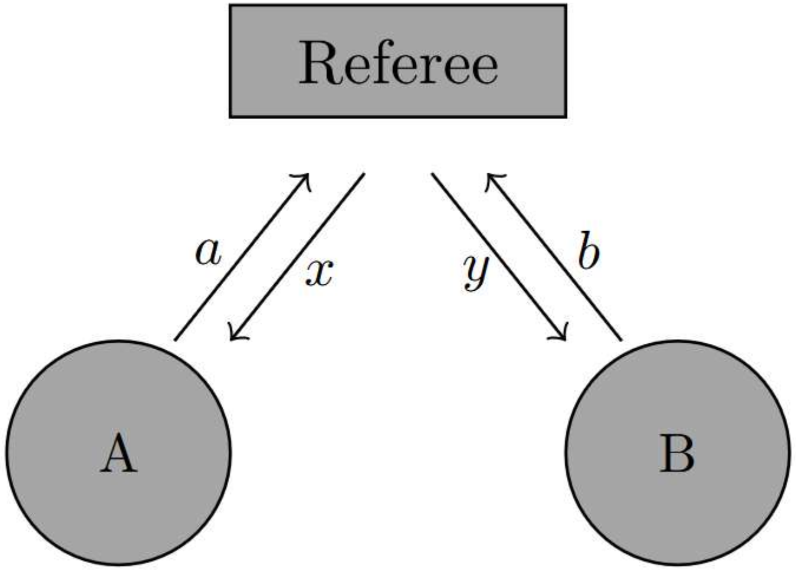


Image source:
"Bertlmann's socks and the nature of reality", Speakable and Unspeakable in Quantum Mechanics by John S. Bell

"Knowledge about one part provides you knowledge about the other."

Entanglement and the CHSH game

1. CHSH game:



- Two distant parties, two measurement settings $x, y \in \{0,1\}$, two outcomes $a, b \in \{0,1\}$ per measurement.
- Correlations: $p(a, b|x, y)$
- Goal: $a \oplus b = x \wedge y$

Entanglement and the CHSH game

3. CHSH game:

- Probability of winning $a \oplus b = x \wedge y$:

$$p_{win} = \sum_{a,b,x,y} p(x)p(y)p(a,b|x,y)\delta_{a\oplus b,x\wedge y} = \frac{1}{4}\sum_{a,b,x,y} p(a,b|x,y)\delta_{a\oplus b,x\wedge y}$$

- Winning conditions:

(x,y)	$a \oplus b$
$(0,0)$	0
$(0,1)$	0
$(1,0)$	0
$(1,1)$	1

Entanglement and the CHSH game

3. CHSH game:

- Classical strategy = probabilistic mixture of deterministic strategies:

$$p(a,b|x,y) = \sum_{\lambda} p(\lambda) p_f(a|x,\lambda) p_g(b|y,\lambda) \Rightarrow p_{win} \leq 0.75$$

- Quantum strategy with entangled state $|\phi^+\rangle_{S_1 S_2} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$p_{win} \approx 0.85$$

Bell's theorem

Statement:

Some predictions of quantum mechanics cannot be explained by a local hidden variable model.

- Local hidden variable model:

$$p(a, b|x, y) = \sum_{\lambda} p(\lambda)p(a|x, \lambda)p(b|y, \lambda)$$

No-cloning theorem

Statement:

There is no quantum operation transforming an ***arbitrary*** *state* $|\psi\rangle$ *to* $|\psi\rangle \otimes |\psi\rangle$.

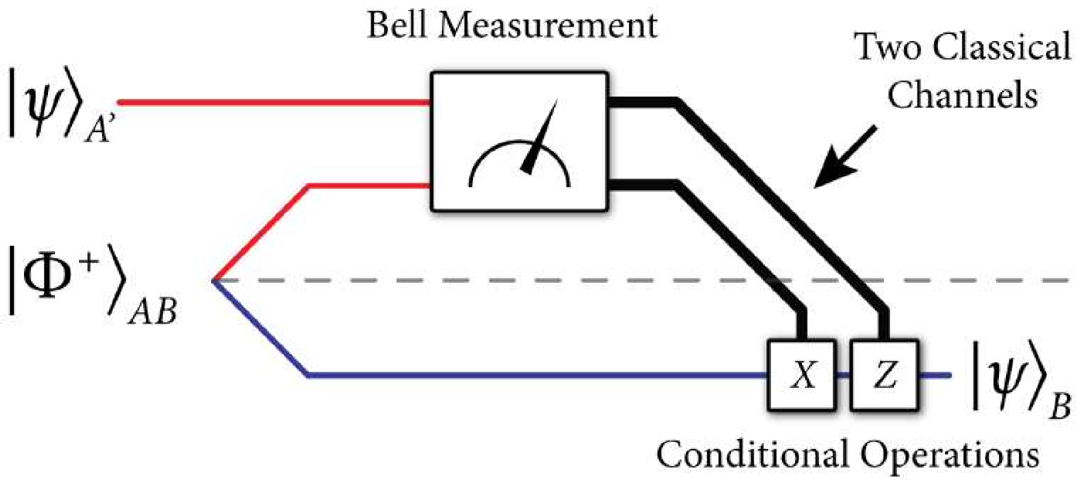
Proof: Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

1. Assume there exists U s.t. $U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$.
2. By linearity of U,

$$\begin{aligned} U(|\psi\rangle|0\rangle) &= U(\alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle) \\ &= \alpha U(|0\rangle|0\rangle) + \beta U(|1\rangle|0\rangle) \\ &= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \\ &\stackrel{?}{=}{}^{*}\ \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = |\psi\rangle|\psi\rangle. \end{aligned}$$

*: Not true in general!

Quantum teleportation



Alice can send her qubit to Bob using shared entanglement and two classical bits

Image source: Wilde, M. M. (2011). From classical to quantum Shannon theory.

Quantum teleportation

- Protocol:

$$|\psi\rangle_{A'AB} = \frac{1}{2}\left[|\phi^+\rangle_{A'A}|\psi\rangle_B + |\phi^-\rangle_{A'A}Z|\psi\rangle_B + |\psi^+\rangle_{A'A}X|\psi\rangle_B + |\psi^+\rangle_{A'A}XZ|\psi\rangle_B\right]$$

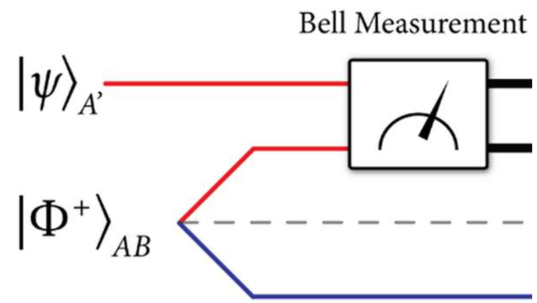
1. Alice measures in the Bell basis and obtains an outcome $a = (x, y) \in \{0, 1\}^2$:

$|\psi\rangle_{A'AB} \to |\phi^+\rangle_{A'A}|\psi\rangle_B$ for $a = (0,0)$

$|\psi\rangle_{A'AB} \to |\phi^-\rangle_{A'A}Z|\psi\rangle_B$ for $a = (0,1)$

$|\psi\rangle_{A'AB} \to |\psi^+\rangle_{A'A}X|\psi\rangle_B$ for $a = (1,0)$

$|\psi\rangle_{A'AB} \to |\psi^-\rangle_{A'A}XZ|\psi\rangle_B$ for $a = (1,1)$



Quantum teleportation

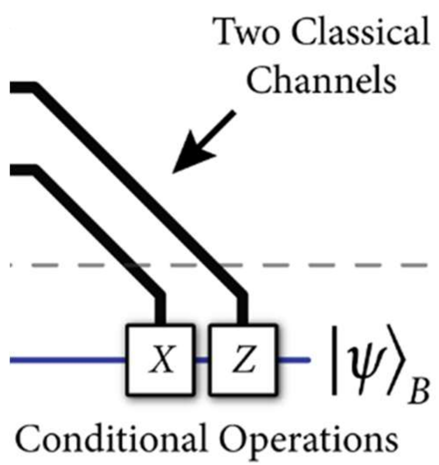
2. She sends her outcome a to Bob, who will then apply the appropriate operation to recover $|\psi\rangle$:

$$|\psi\rangle_B \xrightarrow{X^0 Z^0 = \mathbb{I}} \mathbb{I}|\psi\rangle_B = |\psi\rangle_B \text{ for } a = (0,0)$$

$$Z|\psi\rangle_B \xrightarrow{X^0 Z^1 = Z} Z^2|\psi\rangle_B \text{ for } a = (0,1)$$

$$X|\psi\rangle_\mathrm{B} \xrightarrow{X^1 Z^0 = X} X^2|\psi\rangle_\mathrm{B} = |\psi\rangle_\mathrm{B} \text{ for } a = (1,0)$$

$$XZ|\psi\rangle_B \xrightarrow{X^1 Z^1 = XZ} X^2 Z^2|\psi\rangle_B = |\psi\rangle_B \text{ for } a = (1,1)$$



(by unitarity and hermicity of X and Z, $X^2 = \mathrm{Z}^2 = \mathbb{I}$)

Summary

- Quantum phenomena:

1. Can be leveraged for information-processing tasks (e.g. entanglement for teleportation).
2. Can perform better than classical methods (e.g. entanglement in the CHSH game).

- Limitations on the allowed manipulations (e.g. no-cloning).

Thank you!