I. Introduction

- Goal of Quantum Information (QI):

  Information processing with quantum mechanical systems

  → Notion of information

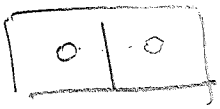
  → Data transmission

  → Computation

  → Implementation

- Why study inf. processing w/ quantum mechanical systems? Isn't information indep. of physical realization?

  Landauer (1961): Erasing information releases heat.



1 particle in box in some position (= 1 bit):
entropy $S_0 = k \ln 2$

erasure →

particle in fixed location (erased information):
entropy $S_1 = 0$.

$$\Rightarrow \Delta S_{sys} = -k \ln 2 \Rightarrow \Delta Q_{dir} = -T \Delta S_{sys} = kT \ln 2$$

$\Rightarrow$ Erasing 1 bit releases $\Delta Q = kT \ln 2$ heat.

$\Rightarrow$ "Information is physical".

(i.e.: We cannot think about information processing w/out its physical realization)

- Moore's Law: # transistors per chip doubles every 18 months

  ⇒ currently ~100 atoms length

  ⇒ quantum effects become important

⇒ Think about how to process information with (not against) quantum mechanics.

Basic Ideas:

- Qubits:

  Classical encoding of information:

  Basic unit: Bit $b = 0, 1$ ← 2 possibilities

  Many bits: Bit string $b_1 \dots b_N = \underbrace{0\dots0, 0\dots01, 0\dots10, \dots \text{etc.}}_{2^N \text{ possibilities}}$

  Quantum information:

  Encode information in quantum bits (qubits)

  Qubit $|b\rangle = |0\rangle, |1\rangle$

  → any superposition possible:

  $$|b\rangle = \alpha|0\rangle + \beta|1\rangle$$

  $\alpha \in \mathbb{C}$, $\beta \in \mathbb{C}$ ← "infinitely many possibilities" (→ cf. Cats!)

Many qubits

$$|b\rangle = \underbrace{\alpha_{0\ldots0}|0\ldots0\rangle + \alpha_{0\ldots01}|0\ldots01\rangle + \alpha_{0\ldots10}|0\ldots10\rangle + \ldots}_{2^N \text{ complex parameters!}}$$

(α: $\mathbb{C}$)

$\Rightarrow$ Many more degrees of freedom / possibilities!

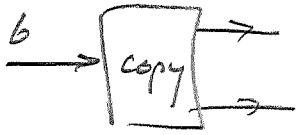
→ Can we store infinitely more information?

→ How can we quantify amount of information?

• Cloning:

Can we copy information?

Classically:



✓

Q. Mech: NO! : incompatible w/ linearity!

Idea:

$$|0\rangle \xrightarrow{\text{copy}} |0\rangle|0\rangle \quad (1)$$

$$|1\rangle \xrightarrow{\text{copy}} |1\rangle|1\rangle \quad (2)$$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \xrightarrow{\text{copy}} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \quad (3)$$

Both/linearity: (1) + (2) $\Rightarrow$

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \xrightarrow{(1),(2)} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$ ↯

"No-cloning theorem": Quantum information cannot be copied!

• Entanglement, teleportation, Bell inequalities:

Consider two parties (= people, labs, quantum systems) Alice (A) and Bob (B).

Consider total state:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B \right)$$

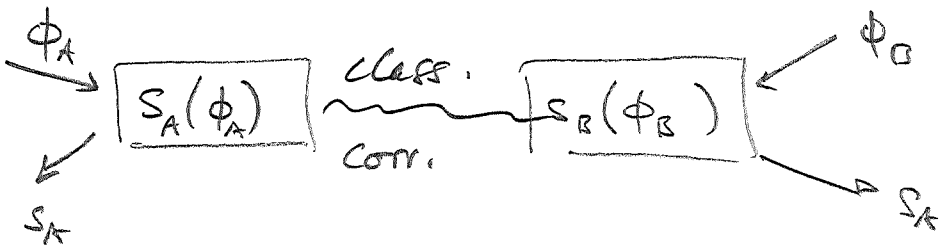
- Alice + Bob measure in $|0\rangle, |1\rangle$ basis
  $\Rightarrow$ their measurement result is anti-correlated!
- In fact, their meas. results in any basis are anti-correlated!

$\Rightarrow$ Parts of the system cannot be described indep.

$\Rightarrow$ Feature of Q. mechanics?

Subtle! (Anti-) correlations can be classical.

E.g., there could be a "true theory of spins" where each spin is described by a classical b.f. for each meas. direction which are all random + anti-correlated:



⇒ Local hidden variable (LHV) model?

⇒ Need more subtle ways to characterize quantumness:
Compare results in different bases!

⇒ Bell inequalities: QM is incompatible with LHV theories!

Teleportation:

Quantum information cannot be cloned: How can we transport it over long distances?

unknown state $|\phi\rangle$ → A B $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ ⊗ C

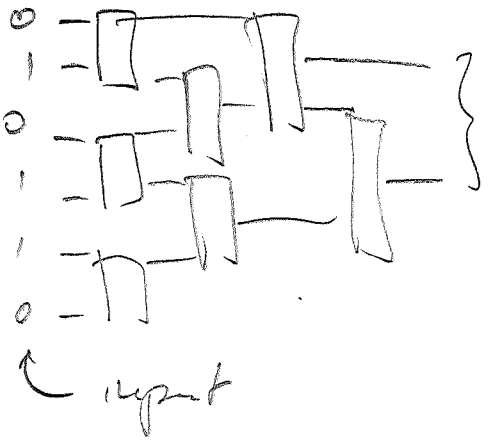
joint measurement → $|\phi\rangle$ "appears" in C,
But we need class. information (meas. outcome) to use it
⇒ no faster than light communication!

Note: Only the state of the quantum system is moved, not the system itself!

(Peres: "disembodied transportation")

• Quantum Computing

Classical computation:



Q. Compute: input can be superposition of exponentially many inputs : exponential speed-up?

Subtle! → Generally not clear how to extract information.

Shor '94: Q. Computer can factor large numbers in time polynomial in # bits (better than best known class. algorithm!)

Error correction:

Noise (random bit flips, ...) can destroy information (esp. at a single-atom/quantum scale!).

→ Error correction!

Classically: copy bit to protect it.

$\hat{0} \longrightarrow 000$

$\hat{1} \longrightarrow 111$

→ protected against flipping 1 bit.

QM: $?: |\hat{0}\rangle \longrightarrow |000\rangle$

$|\hat{1}\rangle \longrightarrow |111\rangle$

Protected against bit flip.

Ref:

$\frac{1}{\sqrt{2}}(|\hat{0}\rangle + |\hat{1}\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

not protected against phase flip: $|0\rangle \rightarrow |0\rangle$

$|1\rangle \longrightarrow -|1\rangle$

⇒ Quantum Error Correction Codes! (QECC).