I. Introduction

- Goal of Quantum Information (QI):
  - Information processing with quantum mechanical systems
  - Nature of information
  - Data transmission
  - Computation
  - Implementation

- Why study info. processes w/ quantum mechanical systems?
  Isn’t information merely a physical realization?

Landauer (1961): Every information release heat.

$$\begin{align*}
\text{A particle in box is} \\
\text{some position (=}1\text{ bit):} \\
\text{entropy } S_k \text{ bit} \leq 2 \\
\rightarrow \Delta S_{\text{sys}} = k \ln 2 \\
\rightarrow \Delta Q_{\text{res}} = -T \Delta S_{\text{sys}} = kT \ln 2 \\
\rightarrow \text{Erasing } 1 \text{ bit releases } \Delta Q = kT \ln 2 \text{ heat.}
\end{align*}$$

"Information is physical."

(i.e. We cannot think about information processing that is physical realization)
* Moore's Law: # transistors per chip doubles every 18 months

\[ \rightarrow \text{ currently } \approx 100 \text{ atoms length} \]

\[ \Rightarrow \text{ quantum effects become important} \]

\[ \Rightarrow \text{ Think about how to process information with (not against) quantum mechanics.} \]

**Basic Ideas:**

- **Quantum**
  - Classical encoding of information:
    - Basic unit: Bit \( b = 0, 1 \Rightarrow 2 \) possibilities
    - Many bits: Bit string \( b_1 \ldots b_n = 0 \ldots 0, 0 \ldots 1, 0 \ldots 10, \ldots \) etc.
      \[ 2^n \text{ possibilities} \]
  
- **Quantum Information**
  - Encode information in quantum bits (qubits)
    - Qubit \( |0\rangle = |0\rangle, |1\rangle \)
    - any superposition possible:
      \[ |0\rangle = \alpha |0\rangle + \beta |1\rangle \]
      \[ \forall \alpha, \beta \in \mathbb{C} \Rightarrow \text{ infinitely many possibilities} \]
      \[ (\Rightarrow \text{ qutrit!}) \]
$|b\rangle = x_{00} |0\ldots0\rangle + x_{01} |0\ldots0\rangle + x_{10} |1\ldots1\rangle + \ldots$

$2^n$ complex parameters!

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

$\Rightarrow$ Can we store infinitely more information?

$\Rightarrow$ How can we quantify amount of information?

@ Cloudy:

Can we copy information?

Classically:

\[ b \xrightarrow{\text{copy}} b \]

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

Idea:

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

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

\[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \xrightarrow{\text{copy}} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \quad (5) \]

By 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-copy theorem": Quantum information cannot be copied!
Consider two parties (= people, labs, quantum systems) Alice (A) and Bob (B).

\[ |\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B) \]

- 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?

Surely! (Anti-) correlations can be classical.

E.g., there could be a "nice theory of spins" described by where each spin is a classical bit for each meas. direction that are all random + anti-correlated!
- Local hidden variable (LHV) models
- 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?

\[
\left| \psi^+ \right> = \frac{1}{\sqrt{2}} \left( |01\rangle + |10\rangle \right)
\]

- Joint measurement
- \( |\psi^+\rangle \) appears in \( C \), but we need classical information (mes, outcome) to use it

**Note:** Only the state of the quantum system is moved, not the particle itself!
(Peres: "disembodied reanimation")
Quantum Computing

Classical computers:

\[
\text{\small \{ input \}} \rightarrow \text{result}
\]

As computers, input can be superposition of exponentially many inputs: exponential speedup?

Sutlej: Generally not clear how to extract information.

Shor '94: Q. Computer can factor large numbers in time polynomial in \( \log n \) (the best known class algorithm!)

Error correction:

Noise (random bit flips, ...) can destroy information (e.g. at a single atom/qubit scale!).
Error correction!

Classically: copy bit to protect it.

\[ \hat{0} \rightarrow 000 \]
\[ \hat{1} \rightarrow 111 \]

→ protected against flipping 1s→0.

QFT: \[ ? : |0\rangle \rightarrow |000\rangle \]
\[ |1\rangle \rightarrow |111\rangle \]

Protected against bit flips.

EPR:

\[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \]

not protected against phase flip: |0\rangle \rightarrow |0\rangle
\[ |1\rangle \rightarrow -|1\rangle \]

→ Quantum Error Correction Codes! (QECC).