I. Introduction

What is Quantum Information Theory?

→ The study of information processing using the laws of quantum mechanics

Quantum mechanics / quantum theory:
The most general framework to describe matter at the fundamental (microscopic) level.

Quantum theories exist for almost all classical physical theories: mechanics (i.e. motion of particles subject to forces), electrodynamics, ... – except gravity.

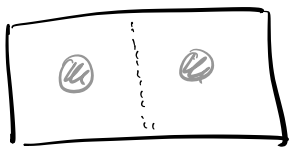
Here, q. mechanics (or q. theory, or q. physics) always refers to the general framework.

Why should we study information processing in the framework of quantum theory?

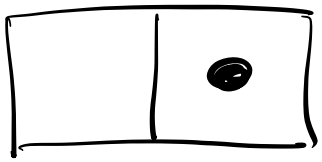
Even further: Why should we study information processing in the context of physics?

Information is a priori a concept unrelated to its physical realization (modern computer, punchcard, relays, paper, ...) – classical information theory (Shannon theory) never talks about physics.

Landauer (1961): Erasing information creates heat:



particle in box at unknown position:
1 bit of information
entropy $S_0 = k \ln 2$



particle in box at known position
bit erased (reset)
entropy $S_1 = 0$

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

$\Rightarrow$ Erasing 1 bit releases $\Delta Q = kT \ln 2$ heat – independent of realization!

Landauer: "Information is physical"

(i.e. we need to take at least the fundamental phys. principles into account when thinking about info. processing in real systems.)

On the other hand: "Moore's Law"

→ # transistors/chip doubles every 18 months

→ transistor size eventually approaches atomic size!

→ must take quantum effects into account:

either fight them or use them.

→ **Quantum Information Theory**

→ Information processing taking into account the fundamental principles of q. theory

— independent of specific physical realization.

Basic principles, ideas, and applications of QI

Classical information: bit $b = 0, 1$

Quantum info: quantum bit (qubit)

with two basis vectors $\vec{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\vec{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

General qubit configuration ("state") is a superposition

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2 \quad , \quad |\alpha|^2 + |\beta|^2 = 1$$

Has similarities to prob. distributions over classical bits,

$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ with $p_0, p_1 \geq 0$, $p_0 + p_1 = 1$, but also

key differences.

"Measurement": Can check (test, measure) the value of a classical bit (e.g. coin in a box) prepared in a state $\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$.

$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ — meas. — prob. p_0 → result "0" ⟶ updated state $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

meas. — prob. p_1 → result "1" ⟶ updated state $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

(2nd measurement gives same result (w.h.p.))

→ measurement "collapses" state.

Measurement of quantum bit:

initial state $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$.

Case a:

$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ → prob. $|\alpha|^2$ → Result "0"

$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ → prob. $|\beta|^2$ → Result "1"

} one possible measurement

But other measurements exist, e.g.:

Case b:

$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ → prob. $\frac{|\alpha+\beta|^2}{2}$ → Result "+"

$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ → prob. $\frac{|\alpha-\beta|^2}{2}$ → Result "−"

Different possibilities can cancel: "Destructive interference"

What is the state after measurement?

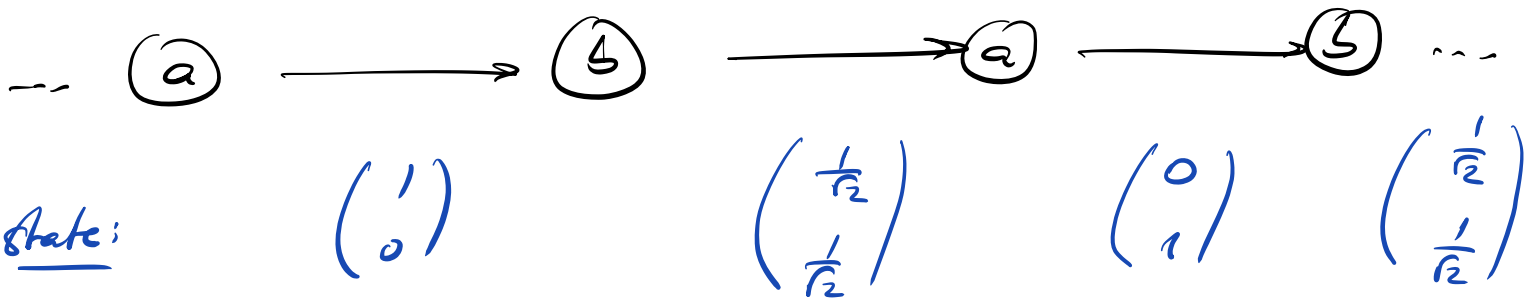
→ same principle: 2× same meas. ⇒ same result!

Case a: State after meas: $\begin{pmatrix}1\\ 0\end{pmatrix}$ or $\begin{pmatrix}0\\ 1\end{pmatrix}$

Case b: State after meas: $\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}$ or $\begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$.

→ State "collapses" onto meas. outcome.

What if we measure



state: $\begin{pmatrix}1\\0\end{pmatrix}$ $\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$ $\begin{pmatrix}0\\1\end{pmatrix}$ $\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}$

prob: $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$

Measuring one "property" can affect others:

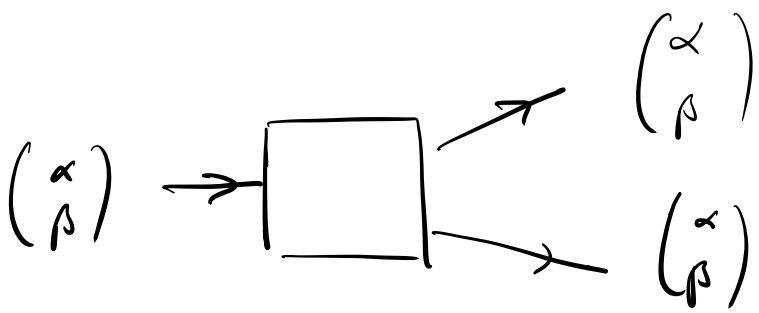
Properties are not independent.

There is no 1-to-1 correspondence between the numbers $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$ and properties we can measure.

Consequences:

- "No-cloning-theorem"

  Quantum information cannot be copied, i.e. a device



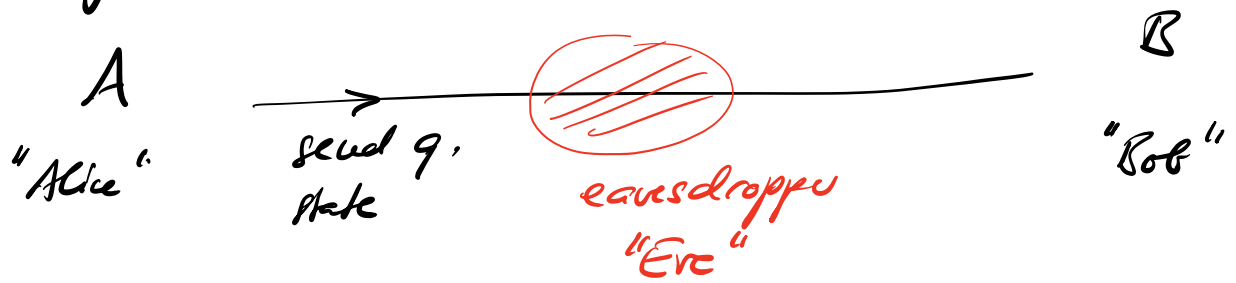
does not exist!

(Otherwise, we could determine $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$ exactly, and measure diff. quantities at the same time.)

(Note: The same holds for class. prob. distributions.)

- Quantum Cryptography

Doing meas. disturbs quantum state:



Measurement disturbs state ⟶
Eve cannot obtain information about state sent without A & B noticing ⟶ can be used to establish secret keys.

- Entanglement, teleportation, Bell inequalities

A & B share joint state: distribution over 00, 01, 10, 11: $\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$ 00 01 10 11

Can choose state such that outcomes are perfectly correlated for all measurements.

This can also happen in a classical theory:
A "hidden variable model" has an independent pre-determined outcome for every test (like a coin).

But: A local hidden variable (LHV) model

where the boxes cannot communicate (→ relativity!)
satisfies special inequalities ("Bell inequalities")
which are violated by quantum states!

→ "Entanglement"

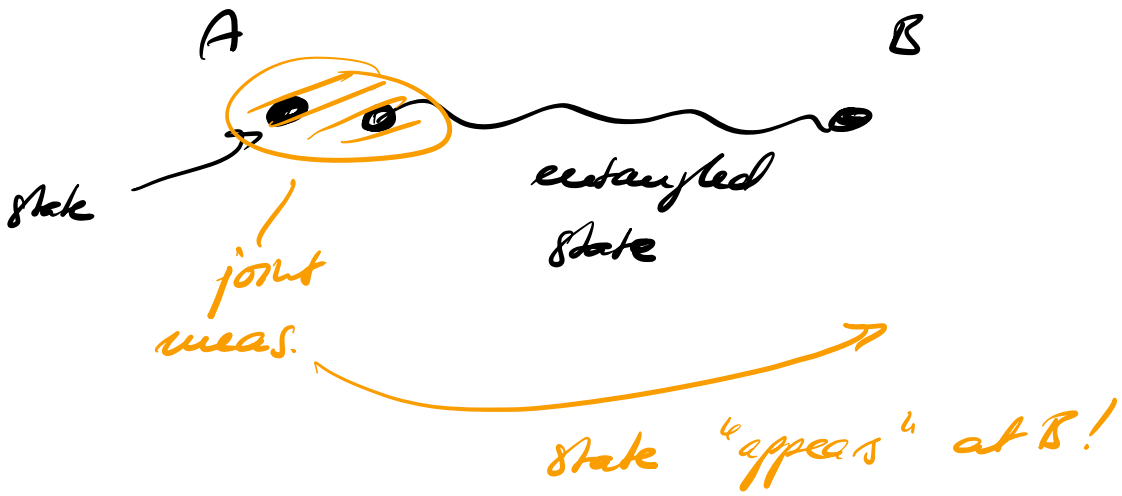
→ Q.M. states can display non-classical correlations

But: No faster-than-light communication possible!!

This also highlights a fundamental difference between probability theory and quantum theory: In prob. th., values are real indep. of measurement, and the state $\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ merely signifies a lack of knowledge.
Quantum theory does not allow for such an interpretation.

Teleportation: A wants to get q, state to B, without risking to lose state. But: No-cloning theorem → A cannot make copies!

→ Teleportation:



→ Does this allow for faster-than-light comm.?

→ No! State on B's side is "scrambled", and requires A's meas. outcome (sent as classical info at speed of light) to be decoded!

Note: The state of the system is teleported, not the system itself.

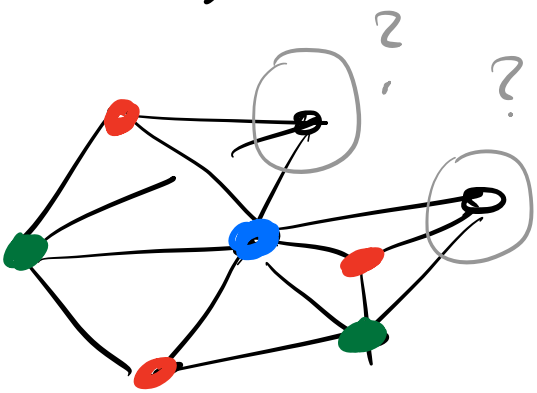
(Asher Peres: "disembodied transportation")

Quantum Computing:

Typical hard computational problem:

"NP problems": Solution may be hard to find, but easy to check.

E.g. graph coloring:



Can we color given graph with e.g. 3 colors s/t same color on adjacent vertices?

Given solution: easy to check!

Quantum computer: Work with quantum bit!

→ Superposition of all possibilities!

→ Might be able to check all solutions at the same time!

→ But: How can we single out the good solutions? Non-trivial problem!

(Note: For class. prob. alg. it also looks like we can test "all possibilities", but there, there's only

describes randomly testing possibilities.

What is different in QI? → Negative numbers!)

Shor '94: Quantum computers can factor numbers exponentially faster than any known classical algorithm.

Quantum Error Correction:

Noise can destroy quantum information!

↑

Any kind of influence from the outside!

How can we protect Q.I. from errors (when storing, transmitting, processing it)?

Classical info: Copy!

$0 \rightarrow 000$ $\quad$ $1 \rightarrow 111$ $\quad$ error, e.g. flip bit 3 $\quad$ 001 $\quad$ 110 $\quad$ correction: maj. vote $\quad$ 0 $\quad$ 1

→ Decreases effective error rate!

Quantum Info: several issues!

- cloning impossible!
- meas. destroys q. state → how to do majority vote?
- errors can be continuous
  → is it ever possible to identify the error?

→ Quantum Error Correction!

Use quantum superpositions to protect quantum superpositions!